K. Nadehara
1/27/04
Q79582
1 of 1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２８日

出願番号
Application Number: 特願２００３－０１８８４５

[ST. 10/C]: [ＪＰ２００３－０１８８４５]

出願人
Applicant(s): 日本電気株式会社

２００３年１０月　２日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００３－３０８１３１４

【書類名】　特許願
【整理番号】　34403229
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/10
　　H03M 13/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　撫原　恒平
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100109313
　【弁理士】
　【氏名又は名称】　机　昌彦
　【電話番号】　03-3454-1111
【選任した代理人】
　【識別番号】　100085268
　【弁理士】
　【氏名又は名称】　河合　信明
　【電話番号】　03-3454-1111
【選任した代理人】
　【識別番号】　100111637
　【弁理士】
　【氏名又は名称】　谷澤　靖久
　【電話番号】　03-3454-1111

【手数料の表示】

【予納台帳番号】　191928

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0213988

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ＡＥＳ暗号処理装置、ＡＥＳ復号処理装置、および、ＡＥＳ暗号・復号処理装置

【特許請求の範囲】

【請求項１】　ステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を暗号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とするＡＥＳ暗号処理装置。

【請求項２】　ＡＥＳ暗号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令を実行するＡＥＳ暗号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とするＡＥＳ暗号処理装置。

【請求項３】　ＡＥＳ暗号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令、排他的論理和演算命令を実行するＡＥＳ暗号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論

理和演算を実行する演算器とを有することを特徴とするＡＥＳ暗号処理装置。

【請求項４】　即値部分が、第０行を指定すると、係数｛０２｝，｛０１｝，｛０１｝，｛０３｝を出力し、第１行を指定すると、係数｛０３｝，｛０２｝，｛０１｝，｛０１｝を出力し、第２行を指定すると、係数｛０１｝，｛０３｝，｛０２｝，｛０１｝を出力し、第３行を指定すると、係数｛０１｝，｛０１｝，｛０３｝，｛０２｝を出力する前記係数テーブルを有することを特徴とする請求項２、または、請求項３記載のＡＥＳ暗号処理装置。

【請求項５】　ステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を復号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とするＡＥＳ復号処理装置。

【請求項６】　ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ復号化命令を実行するＡＥＳ復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とするＡＥＳ復号処理装置。

【請求項７】　ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ復号化命令、排他的論理和演算命令を実行するＡＥＳ復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力

する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とするＡＥＳ復号処理装置。

【請求項８】　即値部分が、第０行を指定すると、係数｛０ｅ｝，｛０９｝，｛０ｄ｝，｛０ｂ｝を出力し、第１行を指定すると、係数｛０ｂ｝，｛０ｅ｝，｛０９｝，｛０ｄ｝を出力し、第２行を指定すると、係数｛０ｄ｝，｛０ｂ｝，｛０ｅ｝，｛０９｝を出力し、第３行を指定すると、係数｛０９｝，｛０ｄ｝，｛０ｂ｝，｛０ｅ｝を出力する前記係数テーブルを有することを特徴とする請求項６、または、請求項７記載のＡＥＳ復号処理装置。

【請求項９】　ステートの１要素を取り出す第１の選択手段と、前記第１の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第１の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第２の選択手段と、前記第２の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第３の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第３の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とするＡＥＳ暗号・復号処理装置。

【請求項１０】　ＡＥＳ暗号化命令、ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令、ＡＥＳ復号化命令を実行するＡＥＳ暗号・復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す第１の選択手段と、前記第１の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第１の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第２の選択手段と、前記第

２の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第３の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第３の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とするＡＥＳ暗号・復号処理装置。

【請求項１１】　ＡＥＳ暗号化命令、ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令、ＡＥＳ復号化命令を実行するＡＥＳ暗号・復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す第１の選択手段と、前記第１の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第１の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第２の選択手段と、前記第２の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第３の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第３の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とするＡＥＳ暗号・復号処理装置。

【請求項１２】　前記第１の選択手段、前記逆アフィン変換回路、前記第２の選択手段、前記逆数換字テーブル、前記アフィン変換回路、第３の選択手段を多重化し、複数列を同時に処理することを特徴とする請求項１０、または、請求項１１記載のＡＥＳ暗号・復号処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＡＥＳ暗号処理装置、ＡＥＳ復号処理装置、および、ＡＥＳ暗号・復号処理装置に関し、特に、所要テーブル容量を削減したＡＥＳ暗号処理装置、ＡＥＳ復号処理装置、および、ＡＥＳ暗号・復号処理装置に関する。

【０００２】

【従来の技術】

光ファイバ、ＡＤＳＬ，ＣＡＴＶなど安価なブロードバンド・インターネット・アクセス手段の普及にともない、インターネット上に暗号で保護された仮想的な通信チャネル（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ，　ＶＰＮ）を用意して高価な専用線を代替し、通信費用の削減を図る動きが加速しつつある。

【０００３】

現在ＶＰＮに用いられている暗号は、５６ｂｉｔ長の共通鍵を用いる米国標準暗号（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ，ＤＥＳ）やその拡張である３ＤＥＳである。しかし、今後は、３ＤＥＳと同等の演算量でより暗号強度が強いと言われている次期米国標準暗号ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号に置き換えられていくと思われる。たとえば、企業の本支店など遠隔地にあるネットワーク間をＶＰＮで結ぶルータにＡＥＳ暗号化機能を実装する方法としては、ＡＥＳ専用ハードウェア・アクセラレータを内蔵する、内蔵マイクロプロセッサに暗号処理専用命令を追加するなどいくつか考えられるが、いずれの場合でも、構成要素として小型かつ高速なＡＥＳ処理回路が必要となる。

【０００４】

以下、ＡＥＳ暗号の概要と従来の実装例を説明する。まず、図２１～図２６を用い、米国の連邦情報処理規格（Ｆｅｄｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｐｒｏｃｅｓｓｉｎｇ　Ｓｔａｎｄａｒｄｓ　Ｐｕｂｌｉｃａｔｉｏｎ，ＦＩＰＳ）１９７（非特許文献１、以下、ＦＩＰＳ１９７と記す）で規定されているＡＥＳの暗号化手順を説明する。

【０００５】

ＡＥＳで用いられるデータ構造である「ステート」を図２１に示す。ＡＥＳでは、入力データを１２８ビット単位のブロックに区切り、１２８，１９２，２５６ビット長の共通鍵で暗号化する。１２８ビット入力は、１６個のバイト（８ビット）データに分解され、４行４列の配列に格納される。この配列を「ステート」と呼ぶ。入力データに対する操作は全てこのステート上で行われる。入力ブロック中の各バイトを早い順にin_0からin_{15}で表すと、図２１（ａ）に示すように、連続したバイトは同一列に格納される。以下の説明では、ステート上の第ｉ行ｊ列の要素を、$S_{i,j}$（$0 \leqq i, j \leqq 3$）と表す（図２１（ｂ））。

【０００６】

ＡＥＳの暗号化処理は非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ５）に疑似コードで示されているが、これをフローチャート化したものを図２２に示す。図２２に示すように、ＡＥＳ暗号化では、「ラウンド（１４０３）」と呼ばれるひとまとまりの処理を繰り返すことで暗号化する。ラウンドの回数（Ｎｒ）は鍵長により決まり、鍵長が１２８，１９２，２５６ビット時のラウンドの回数はそれぞれ１０，１２，１４回である。原則としてラウンドはＳｕｂＢｙｔｅｓ（１４０４，バイト置換）、ＳｈｉｆｔＲｏｗｓ（１４０５，同一行内のシフト），ＭｉｘＣｏｌｕｍｎｓ（１４０６，同一列内の相互演算），ＡｄｄＲｏｕｎｄＫｅｙ（１４０７，拡大鍵の加算）から構成される。ただし、第１ラウンドの前にもＡｄｄＲｏｕｎｄＫｅｙがあり（１４０２）、最終ラウンド１４０８にＭｉｘＣｏｌｕｍｎｓはない。以下単に「ラウンド」と表記するときは、最終ラウンド以外のラウンドを指すこととする。

【０００７】

ラウンドを構成する各処理について説明する。ＳｕｂＢｙｔｅｓ１４０４は、ステート上の各要素を１バイト入出力の換字テーブルにより１対１に変換する処理である。８ビット２５６語の換字テーブルの内容は、非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ７）で与えられているが、数学的には、入力値のガロア体ＧＦ（2^8）上の逆数をとり、その結果にビット間の排他的論理和によるアフィン変換（非特許文献１（ＦＩＰＳ１９７，式（５．１）、または、式（５．２）

））を施した結果を予め計算しておいたものである。以下、この換字テーブルを、非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ７）のキャプションにならいＳ－ｂｏｘと記す。ＳｈｉｆｔＲｏｗｓ１４０５は、同一行内のシフト処理である。第ｉ行（０≦ｉ≦３）の４要素をｉ要素左ローテイト処理する。ＭｉｘＣｏｌｕｍｎｓ１４０６では、非特許文献１（ＦＩＰＳ１９７，式（５．６））で与えられている係数を用い、同一行内で積和演算（乗算と加算）処理を行う。ＡｄｄＲｏｕｎｄＫｅｙ１４０７は、共通鍵から生成した拡大鍵を加算する。ここで、ＭｉｘＣｏｌｕｍｎｓで用いる乗算と加算、ＡｄｄＲｏｕｎｄＫｅｙで用いる加算は、ガロア体ＧＦ（２^{8}）上で８ビットの数値間に定義された演算を用いる。ガロア体ＧＦ（２^{8}）上の加算はビットごとの排他的論理和で行えるため加算器はゲート数個で構成できるが、ガロア体乗算器を構成するには数十ゲート必要である。

【０００８】

ラウンドを構成する処理のうち、ＳｕｂＢｙｔｅｓ１４０４，ＳｈｉｆｔＲｏｗｓ１４０５，ＭｉｘＣｏｌｕｍｎｓ１４０６処理を高速化する従来の技術を説明する。これら３つの処理に注目するのは、ＳｕｂＢｙｔｅｓは、テーブル参照を多く含み、またＭｉｘＣｏｌｕｍｎｓは、ガロア体ＧＦ（２^{8}）上の乗算を多く含むために実装方法によっては演算量を要求すること、またＳｈｉｆｔＲｏｗｓはＳｕｂＢｙｔｅｓと一体化して処理できることによる。一方、ＡｄｄＲｏｕｎｄＫｅｙは単純であり独立性が高いので、別に処理しても問題がない。

【０００９】

ＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ処理を一体化したシグナルフローを図２３に示す。この図には、ステートを構成する１６要素のうち、１列分４要素のラウンド処理結果を出力するためのシグナルフローを示してある。従って、ステートの全１６要素（４列）について１ラウンド分の結果を得るには、図２３に示したのと同等の演算を、ステート上の入出力位置をシフトしながら合計４回繰り返す必要がある。なお、図２３において、ＳｕｂＢｙｔｅｓ１５０１とＳｈｉｆｔＲｏｗｓとの処理順序は入れ替えてある。ＳｕｂＢｙｔｅｓは場所を保存したまま値を変える処理、ＳｈｉｆｔＲｏｗｓは値を保存し

たまま場所を変える処理なので、順序を入れ替えても同一の結果が得られる。また、ＳｈｉｆｔＲｏｗｓは、ＳｕｂＢｙｔｅｓの各入力の取得位置を指定する操作で実現されている。ＭｉｘＣｏｌｕｍｎｓでは、各Ｓ－ｂｏｘ出力に個別に係数を乗算１５０２したうえで加算１５０３する。係数の値は、非特許文献１（ＦＩＰＳ１９７，式（５．６））に示された通りである。ここで、ＧＦ（２８）上の係数との乗算であることを明示するため、非特許文献１（ＦＩＰＳ１９７，４章）での記述にならい「・｛１６進数｝」と表記してある。

【００１０】

次に、ＡＥＳラウンド処理の高速ハードウェア実装手法について説明する。

【００１１】

従来の高速化手法としては、複数のＳ－ｂｏｘを用意し並列処理することが行われてきた。たとえば、非特許文献２では、同一内容のＳ－ｂｏｘを１６個用意し、ステートの全１６要素を同時に処理している。類似例では、非特許文献３でも、ＡＥＳに選定されたＲｉｊｎｄａｅｌのデータブロック長１２８ビット・モードにおいては、同一内容のＳ－ｂｏｘを１６個用意し、ステート上の全１６要素を同時に処理している。

【００１２】

さらに、並列度を上げた例として、非特許文献４がある。非特許文献４において、ＭｃＬｏｏｎｅらは、ステートの全１６要素分、かつ１２８ｂｉｔ鍵時の全１０ラウンド分のハードウェアを用意し並列処理しているが、そこから図２３に対応する１ラウンド４要素分のＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ処理回路を抜き出したものを図２４に示す。図２４に示したように、Ｓ－ｂｏｘの内容を定数倍する代わりに予め係数倍した内容を格納したＳ－ｂｏｘを係数の種類だけ用意し、ガロア体乗算器１５０２を不要としている。具体的には、Ｓ－ｂｏｘ出力を｛０２｝，｛０３｝倍する代わりに、Ｓ－ｂｏｘをそのまま実装したテーブルに加え、Ｓ－ｂｏｘテーブル上の各値を｛０２｝，｛０３｝倍した値を格納したテーブルも用意している。

【００１３】

このように、既存のハードウェア実装ではＳ－ｂｏｘの容量を増やすことで並

〃列度〃を上げ、〃高速化を図ってきた。

【００１４】

次に、大容量テーブルを使ったＡＥＳラウンド処理の高速ソフトウェア実装手法について説明する。

【００１５】

非特許文献５に、市販マイクロプロセッサ上のアセンブリ言語でＡＥＳを実装したソースコード例ａｅｓｃｒｙｐｔ．ａｓｍがある。ここでは、図２５に示すシグナルフロー図に従った演算が行われている。

【００１６】

この手法では、８ビット２５６語のＳ－ｂｏｘ（１５０１，１６０１）の代わりに、３２ビット２５６語の拡張Ｓ－ｂｏｘ０，拡張Ｓ－ｂｏｘ１，拡張Ｓ－ｂｏｘ２，拡張Ｓ－ｂｏｘ３を予め計算し主記憶上に保持しておく（１７０１）。テーブル中のすべての語について、拡張Ｓ－ｂｏｘ０ではビット０～７，８～１５，１６～２３，２４～３１に、同じインデックス位置のＳ－ｂｏｘテーブル値をそれぞれ｛０２｝，｛０１｝，｛０１｝，｛０３｝倍した値を格納しておく。同様にテーブル各出力の、ビット０～７，８～１５，１６～２３，２４～３１に、同じインデックス位置のＳ－ｂｏｘ値を、拡張Ｓ－ｂｏｘ１ではそれぞれ｛０３｝，｛０２｝，｛０１｝，｛０１｝倍した値を、拡張Ｓ－ｂｏｘ２ではそれぞれ｛０１｝，｛０３｝，｛０２｝，｛０１｝倍した値を、拡張Ｓ－ｂｏｘ３ではそれぞれ｛０１｝，｛０１｝，｛０３｝，｛０２｝倍した値を格納しておく。このような拡張Ｓ－ｂｏｘ０～３を用意すれば、４回の拡張Ｓ－ｂｏｘ読み出し１７０２と、４回のＧＦ（２^{8}）上の加算１７０３で図２３と同等のシグナルフローが実現でき、１ラウンド１列（４要素）分のＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ処理が行える。

【００１７】

非特許文献５の方法（Ｇｌａｄｍａｎの方法）は、１個の３２ビット長レジスタに８ビット長の要素を４個パックして４並列ＳＩＭＤ（Ｓｉｎｇｌｅ　Ｉｎｓｔｒｕｃｔｉｏｎ　Ｍｕｌｔｉｐｌｅ　Ｄａｔａ）演算を行うため高速である。

【００１８】

最後に、ＡＥＳ復号化について述べる。

【００１９】

ＡＥＳ復号化は、非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ１５）に疑似コードで示されているが、これをフローチャート化したものを図２６に示す。

【００２０】

ここで、ＩｎｖＳｕｂＢｙｔｅｓ１８０４は、ＳｕｂＢｙｔｅｓ１４０４の逆処理、ＩｎｖＳｈｉｆｔＲｏｗｓ１８０５は、ＳｈｉｆｔＲｏｗｓ１４０５の逆処理、ＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６は、ＭｉｘＣｏｌｕｍｎｓ１４０６の逆処理である。ＡｄｄＲｏｕｎｄＫｅｙ１４０７の逆処理はＡｄｄＲｏｕｎｄＫｅｙ自身であるが、区別のためＡｄｄＲｏｕｎｄＫｅｙ’１８０７と表記してある。

【００２１】

復号化は、単純に暗号化の逆処理である。ただし、図２６に示した復号化では、図２２に示した暗号化の各処理を逆順に行うだけでなく、次に述べるように処理順序の最適化を施している。まず、ＩｎｖＳｈｉｆｔＲｏｗｓ１８０５とＩｎｖＳｕｂＢｙｔｅｓ１８０４とを入れ替えている。ＩｎｖＳｈｉｆｔＲｏｗｓ１８０５は、値を保ったまま場所を変える処理であり、ＩｎｖＳｕｂＢｙｔｅｓ１８０４は、場所を保ったまま値を変える処理なので、順番を入れ替えても結果は同一である。

【００２２】

次に、ＡｄｄＲｏｕｎｄＫｅｙ’１８０７とＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６を入れ替えている。ＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６は、線形処理なので、本来、ＡｄｄＲｏｕｎｄＫｅｙ’１８０７の出力に、ＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６を施すべきところ、ＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６の出力に、ＡｄｄＲｏｕｎｄＫｅｙ’１８０７を施しても同一の結果が得られる。

【００２３】

ただし、順序を入れ替えたＡｄｄＲｏｕｎｄＫｅｙ’１８０７では、暗号化時と同じ拡大鍵ではなく、ＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６を施した拡大鍵を使う必要がある。

【００２４】

ＡＥＳ暗号化処理のフローチャート図２２と復号化処理のフローチャート図２６を比較すると、ラウンド内の処理は暗号化と復号化で良く似ていることがわかる。違いはＳｕｂＢｙｔｅｓ１４０４とＩｎｖＳｕｂＢｙｔｅｓ１８０４で用いる換字テーブルの内容とＭｉｘＣｏｌｕｍｎｓ１４０６とＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６で用いる係数である。ＩｎｖＳｕｂＢｙｔｅｓ１８０４ではＦＩＰＳ１９７，Ｆｉｇｕｒｅ１４で示されている換字テーブル（以下ＩｎｖｅｒｓｅＳ－ｂｏｘ）を、ＩｎｖＭｉｘＣｏｌｕｍｎｓ１８０６ではＦＩＰＳ１９７，式（５．１０）で与えられている係数を用いる。

【００２５】

ＡＥＳ復号化の実装を説明する。暗号化と復号化のフローチャートは似ているので、図２４に示したＭｃＬｏｏｎｅらの方法を復号化のうちＩｎｖＳｕｂＢｙｔｅｓ１８０４，ＩｎｖＳｈｉｆｔＲｏｗｓ１８０５，ＩｎｖＭｉｘＣｏｌｏｍｎｓ１８０６の高速処理に適用できる。この場合、１ラウンド１列あたりＩｎｖＳｂｏｘの内容を｛０９｝，｛０ｂ｝，｛０ｄ｝，｛０ｅ｝倍した４種類のテーブルを要素ごとに用意する、すなわち８ビット２５６語のテーブルを１列あたり１６個、１ラウンド１要素あたりに換算して４個（８Ｋビット）使用する。これらの復号化に用いるテーブルは、暗号化とは共用できない。

【００２６】

図２５に示したＧｌａｄｍａｎの方法も復号化ＩｎｖＳｕｂＢｙｔｅｓ１８０４，ＩｎｖＳｈｉｆｔＲｏｗｓ１８０５，ＩｎｖＭｉｘＣｏｌｏｍｎｓ１８０６の高速処理に適用できる。この場合、暗号化と同様、復号化でも１ラウンド１列あたり３２ビット２５６語のテーブルを４個（３２ｋビット）用意しなければならない。これらの復号化に用いるテーブルは、暗号化とは共用できない。

【００２７】

また、ガロア体上の演算器を利用する技術としては、特許文献１記載の技術がある。

【００２８】

【特許文献１】

特開2.０００－３２２２８０号公報

【非特許文献１】

連邦情報処理規格（Ｆｅｄｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｐｒｏｃｅｓｓｉｎｇ　Ｓｔａｎｄａｒｄｓ　Ｐｕｂｌｉｃａｔｉｏｎ）、ＦＩＰＳ１９７、（米国）

【非特許文献２】

清家秀律ほか、「ＦＰＧＡを用いたＡＥＳ暗号の試作」、電子情報通信学会技術報告、ＶＬＤ２００１－９１，ＩＣＤ２００１－３５，ＦＴＳ２００１－３８，２００１年１１月

【非特許文献３】

Ｐａｔｒｉｃｋ　Ｒ．　Ｓｃｈａｕｍｏｎｔほか、“Ｕｎｌｏｃｋｉｎｇ　ｔｈｅ　Ｄｅｓｉｇｎ　Ｓｅｃｒｅｔｓ　ｏｆ　ａ　２．２９　Ｇｂ／ｓ　Ｒｉｊｎｄａｅｌ　Ｐｒｏｃｅｓｓｏｒ”，Ｐｒｏｃ．　３９ｔｈ　Ｄｅｓｉｇｎ　Ａｕｔｏｍａｔｉｏｎ　Ｃｏｎｆｅｒｅｎｃｅ，講演番号４１．１，Ｊｕｎｅ　２００２

【非特許文献４】

Ｍ．　ＭｃＬｏｏｎｅほか、“Ｒｉｊｎｄａｅｌ　ＦＰＧＡ　Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ　Ｕｔｉｌｉｚｉｎｇ　Ｌｏｏｋ－Ｕｐ　Ｔａｂｌｅｓ”，ＩＥＥＥ　Ｗｏｒｋｓｈｏｐ　ｏｎ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｓｙｓｔｅｍｓ，　２００１年，ｐ．３４９～ｐ．３６０

【非特許文献５】

Ｂｒｉａｎ　Ｇｌａｄｍａｎ、ソフトウェア・アーカイブａｅｓｓｒｃ．ｚｉｐ、［ｏｎｌｉｎｅ］、［平成１５年１月１０日検索］、インターネット＜ｈｔｔｐ：／／ｆｐ．ｇｌａｄｍａｎ．ｐｌｕｓ．ｃｏｍ／ｃｒｙｐｔｏｇｒａｐｈｙ＿ｔｅｃｈｎｏｌｏｇｙ／ｒｉｊｎｄａｅｌ／＞

【００２９】

【発明が解決しようとする課題】

非特許文献２の方法では、暗号化のために１ラウンドあたり８ビット２５６語のテーブル１６個、計３２ｋビットを用意し、ステート上の全１６要素を同時に

計算している。１ラウンド１要素あたりに換算すれば２ｋビットのテーブルを使用している。

【００３０】

非特許文献４の方法では、暗号化のために１６０１のようにステート１列あたり８ビット２５６語のテーブルを１２個（２４ｋビット）、１ラウンド１要素あたりに換算して３個（６ｋビット）使用している。復号化のためには８ビット２５６語のテーブルを１６個（３２ｋビット）、１ラウンド１要素あたりに換算して４個（８ｋビット）使用する。

【００３１】

非特許文献５の方法では、暗号化のために、３２ビット２５６語のテーブルを４個（３２ｋビット）用意する必要がある。１ラウンド１要素あたりに換算すれば、８ｋビット使用している。復号化のためにも同じく３２ビット２５６語のテーブルを４個（３２ｋビット）、１ラウンド１要素あたりに換算すれば、８ｋビットのテーブルを用意する必要がある。

【００３２】

このように、従来の技術では、処理に用いるテーブル容量を増やすことで高速化を図ってきた。しかし、テーブル容量の増加はＡＥＳ演算器のハードウェア規模の増大に直結する。たとえば、非特許文献４の方法では、ガロア体乗算器を削除する替わりに、Ｓ－ｂｏｘテーブルの個数を増やしているが、ガロア体乗算器は、数十ゲート規模で構成できるのに対し、８ビット２５６語のＳ－ｂｏｘテーブルは、数千～１万ゲート規模もあるため、高速化の代償としてハードウェア規模が飛躍的に増えている。しかし、高速化は重要だが、ハードウェア規模が増大するのでは実用的とはいえない。

【００３３】

同様、特許文献１にも、効果的なハードウェア量削減の技術は、開示されていない。

【００３４】

本発明の目的は、処理性能を保ちつつ、Ｓ－ｂｏｘテーブル容量を削減した、小型かつコストパフォーマンスの良いＡＥＳ暗号処理装置を実現することである

【００３５】

【課題を解決するための手段】

本発明の第１のＡＥＳ暗号処理装置は、ステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を暗号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とする。

【００３６】

本発明の第２のＡＥＳ暗号処理装置は、ＡＥＳ暗号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令を実行するＡＥＳ暗号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする。

【００３７】

本発明の第３のＡＥＳ暗号処理装置は、ＡＥＳ暗号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令、排他的論理和演算命令を実行するＡＥＳ暗号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガ

ロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする。

【００３８】

本発明の第４のＡＥＳ暗号処理装置は、前記第２、または、第３のＡＥＳ暗号処理装置であって、即値部分が、第０行を指定すると、係数｛０２｝，｛０１｝，｛０１｝，｛０３｝を出力し、第１行を指定すると、係数｛０３｝，｛０２｝，｛０１｝，｛０１｝を出力し、第２行を指定すると、係数｛０１｝，｛０３｝，｛０２｝，｛０１｝を出力し、第３行を指定すると、係数｛０１｝，｛０１｝，｛０３｝，｛０２｝を出力する前記係数テーブルを有することを特徴とする。

【００３９】

本発明の第１のＡＥＳ復号処理装置は、ステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を復号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とする。

【００４０】

本発明の第２のＡＥＳ復号処理装置は、ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ復号化命令を実行するＡＥＳ復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする。

【００４１】

本発明の第３のＡＥＳ復号処理装置は、ＡＥＳ復号化命令であることを示す部

分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ復号化命令、排他的論理和演算命令を実行するＡＥＳ復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい４個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする。

【００４２】

本発明の第４のＡＥＳ復号処理装置は、前記第２、または、第３のＡＥＳ復号処理装置であって、即値部分が、第０行を指定すると、係数｛０ｅ｝，｛０９｝，｛０ｄ｝，｛０ｂ｝を出力し、第１行を指定すると、係数｛０ｂ｝，｛０ｅ｝，｛０９｝，｛０ｄ｝を出力し、第２行を指定すると、係数｛０ｄ｝，｛０ｂ｝，｛０ｅ｝，｛０９｝を出力し、第３行を指定すると、係数｛０９｝，｛０ｄ｝，｛０ｂ｝，｛０ｅ｝を出力する前記係数テーブルを有することを特徴とする。

【００４３】

本発明の第１のＡＥＳ暗号・復号処理装置は、ステートの１要素を取り出す第１の選択手段と、前記第１の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第１の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第２の選択手段と、前記第２の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第３の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第３の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とする。

【００４４】

本発明の第２のＡＥＳ暗号・復号処理装置は、ＡＥＳ暗号化命令、ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令、ＡＥＳ復号化命令を実行するＡＥＳ暗号・復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す第１の選択手段と、前記第１の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第１の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第２の選択手段と、前記第２の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第３の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第３の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする。

【００４５】

本発明の第３のＡＥＳ暗号・復号処理装置は、ＡＥＳ暗号化命令、ＡＥＳ復号化命令であることを示す部分、入力レジスタを指定する第１オペランド部分、出力レジスタを指定する第２オペランド部分、行を指定する即値部分を含むＡＥＳ暗号化命令、ＡＥＳ復号化命令を実行するＡＥＳ暗号・復号処理装置であって、第１オペランド部分、即値部分にしたがい前記入力レジスタからステートの１要素を取り出す第１の選択手段と、前記第１の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第１の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第２の選択手段と、前記第２の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第３の選択手段と、選択された要

素の行に応じた係数を出力する係数テーブルと、前記第３の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第２オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする。

【００４６】

本発明の第４のＡＥＳ暗号・復号処理装置は、前記第２、または、第３のＡＥＳ暗号・復号処理装置であって、前記第１の選択手段、前記逆アフィン変換回路、前記第２の選択手段、前記逆数換字テーブル、前記アフィン変換回路、第３の選択手段を多重化し、複数列を同時に処理することを特徴とする。

【００４７】

【発明の実施の形態】

ＡＥＳでは、ガロア体（Ｇａｌｏｉｓ　ｆｉｅｌｄ，ＧＦ）上の演算を、アルゴリズムの定義に用いている。

【００４８】

まず、ＧＦ（2^8）上の数について説明する。

【００４９】

一般に、ＧＦ（ｐ）上の元を係数とするｍ次の多項式は、既約多項式（ｉｒｒｅｄｕｃｉｂｌｅ　ｐｏｌｙｎｏｍｉｎａｌ）を法とする加算と乗算について体をなし、この体をＧＦ（p^m）と表記する。ＧＦ（2^8）上の多項式は、一般に次のように書ける。

【００５０】

$$b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0 \quad (1)$$

【００５１】

ここで、b_i（$0 \leqq i \leqq 7$）は、ガロア体ＧＦ（２）上の要素なので、０か１である。式（１）は、係数のみ取り出し｛$b_7b_6b_5b_4b_3b_2b_1b_0$｝とベクトル表現でも書ける。かっこ内部を１６進表記することもある。

【００５２】

ＧＦ（2^8）上には３０個余りの既約多項式があるが、ＡＥＳでは次式（２）

"を採用している。"

【００５３】

$m(x)=x^8+x^4+x^3+x+1$　（２）。

【００５４】

次に、ＡＥＳにおけるＧＦ（2^8）上の加算について説明する。

【００５５】

ＧＦ（2^8）上の加算は、ベクトル表現された数のビットごとの排他的論理和（ＸＯＲ）をとるだけでよい。すなわち、｜$a_7a_6a_5a_4a_3a_2a_1a_0$｜と｜$b_7b_6b_5b_4b_3b_2b_1b_0$｜との和｜$c_7c_6c_5c_4c_3c_2c_1c_0$｜は次式（３）で表される。多項式の加算は、同次数の係数どうしを加算すればよく、ＧＦ（２）上の加算は排他的論理和（ＸＯＲ）だからである。ここで、＜ＸＯＲ＞は、排他的論理和を示す。

【００５６】

$c_i=a_i<XOR>b_i$　$(0\leqq i\leqq 7)$　（３）。

【００５７】

図１３は、ガロア体ＧＦ（2^8）上の加算器の例を示すブロック図である。

【００５８】

図１３を参照すると、ハードウェアによるＧＦ（2^8）上の加算器は、ＸＯＲゲート８個で簡単に構成できる。通常の２進数とは異なり、桁上げ処理は不要である。

【００５９】

次に、ＡＥＳにおけるＧＦ（2^8）上の乗算について説明する。

【００６０】

図１４は、ガロア体ＧＦ（2^8）上の２倍回路の例を示すブロック図である。

【００６１】

乗算は、被乗数の２のべき乗倍と加算の組み合わせで実現する。まず、入力を２倍する方法を説明する。式（１）を２＝｜００００００１０｜倍することは、ｘ倍することに等しいので、次式（５）で表せる。これは、ベクトル表現を左１ｂｉｔシフトすることに等しい。

【００６２】

$b_7x^8+b_6x^7+b_5x^6+b_4x^5+b_3x^4+b_1x^3+b_1x^2+b_0x^1$（５）。

【００６３】

次に、この式（５）を、式（２）で定義したｍ（ｘ）に対して既約にする。$b_7=0$ならば既約であるが、$b_7=1$の場合は既約ではないので、式（５）からｍ（ｘ）を減算する、すなわち、｛１ｂ｝＝｛０００１１０１１｝とＸＯＲする必要がある。この一連の操作は、たとえば、図１４に示した回路で行える。

【００６４】

任意の数との乗算は、部分積を発生する２倍回路とＡＮＤゲート、部分積を加算する回路の組み合わせで実現できる。

【００６５】

図１５は、ガロア体ＧＦ（2^8）上のガロア体乗算器の例を示すブロック図である。

図１５において、「２×」は、図１４の２倍回路を示す。また、「ＸＯＲ」は、図１３の加算器である。実装方法にもよるが、暗号化時は｛０２｝、｛０３｝倍の回路が必要になる。復号化時は｛０９｝、｛０ｂ｝、｛０ｄ｝、｛０ｅ｝倍の回路が必要になる。

【００６６】

次に、本発明の第１の実施の形態について図面を参照して詳細に説明する。

【００６７】

図１は、本発明の第１の実施の形態の構成を示すブロック図である。

【００６８】

図１を参照すると、本発明の第１の発明の実施の形態は、入力ステート１０１と、列マルチプレクサ１０２と、演算入力レジスタ１０３と、行マルチプレクサ１０４と、Ｓ－ｂｏｘテーブル１０５と、係数テーブル１０６と、ガロア体ＧＦ（2^8）上のガロア体乗算器１０７と、演算結果レジスタ１０８と、ガロア体加算器１０９と、累算レジスタ１１０とから構成されるＡＥＳ暗号化装置である。また、演算入力レジスタ１０３、行マルチプレクサ１０４、Ｓ－ｂｏｘテーブル

１０５、係数テーブル１０６、ガロア体ＧＦ（２^{8}）上のガロア体乗算器１０７、および、演算結果レジスタ１０８を含む部分をＡＥＳ暗号回路１１１とする。

【００６９】

ガロア体ＧＦ（２^{8}）上のガロア体乗算器１０７は、図１５に示すものであり、図１５のb_7～b_0には、Ｓ－ｂｏｘテーブル１０５の出力８ビットが入力され、a_1～a_0には、係数テーブル１０６の出力２ビット（たとえば、図２の行指定０の整数１の｛０１｝を示す２ビット“０１”）が接続される。a_7～a_2の部分の回路は、設けなくてよい。ガロア体ＧＦ（２^{8}）上のガロア体乗算器１０７には、図１５の乗算器が４個設けられる。

【００７０】

演算入力レジスタ１０３、演算結果レジスタ１０８は、遅延時間、パイプライン制御等を考慮したものであり、必ずしも必要はない。

【００７１】

入力ステート１０１は、$S_{0,0}$～$S_{3,3}$の１６個の要素（データ）であり、それぞれの要素は、８ビットである。また、たとえば、入力ステート１０１の１列ずつが、ソフトウェア可視のレジスタに格納される。

【００７２】

列マルチプレクサ１０２は、４列ある入力ステート１０１から指定された１列４要素を選択し出力する。演算入力レジスタ１０３は、列マルチプレクサ１０２の出力である１列４要素を保持する。行マルチプレクサ１０４は、入力レジスタ１０３の４要素から指定された行にある１要素（８ビット）を選択し出力する。Ｓ－ｂｏｘテーブル１０５は、行マルチプレクサ１０４の出力（８ビット）をインデックスとして８ビットのデータを出力する。Ｓ－ｂｏｘテーブル１０５は、たとえば、２５６語×８ビットのＲＯＭ、ＲＡＭ、または、組み合わせ回路等で構成される。

【００７３】

Ｓ－ｂｏｘテーブル１０５の出力は、ＧＦ（２^{8}）上のガロア体乗算器１０７（４個の部分乗算器を含む）に入力される。各部分乗算器には、行指定に従って、係数テーブル１０６から係数が供給され、ＧＦ（２^{8}）上の乗算が実行される

。演算結果レジスタ１０８は、ＧＦ（２８）上のガロア体乗算器１０７の出力の連結された４×８ビットのデータを格納する。ガロア体加算器１０９は、演算結果レジスタ１０８の４×８ビットの値と累算レジスタ１１０上の値とのＧＦ（２８）上の加算を実行する。累算レジスタ１１０は、ガロア体加算器１０９の出力（４×８ビット）を格納する。このようにして、ステート１列分のＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ処理のうち１／４（１要素分）が完了する。

【００７４】

図１６は、図１のＳ－ｂｏｘテーブル１０５の内容を示す説明図である。

【００７５】

図１６を参照すると、Ｓ－ｂｏｘテーブル１０５の内容は、非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ７）に示されているものであり、たとえば、インデックスが、｛ｂ３｝であれば、内容は、｛６ｄ｝である。

【００７６】

図２は、図１の係数テーブル１０６の内容を示す説明図である。

【００７７】

図２を参照すると、係数テーブル１０６の内容は、非特許文献１（ＦＩＰＳ１９７，式（５．６））に示される係数行列を転置したものである。

【００７８】

次に、本発明の第１の実施の形態の動作について図面を参照して詳細に説明する。

【００７９】

図３は、本発明の第１の実施の形態の動作を示す説明図である。

【００８０】

図３を参照すると、事前に累算レジスタ１１０をゼロクリアしておく（図３Ｓ３０１）。まず、第０列、第０行を処理する。列マルチプレクサ１０２はステート１０１から第０列を選択、出力する（図３Ｓ３０２）。その中から行マルチプレクサ１０４は、第０行のＳ０，０を選択、出力する（図３Ｓ３０３）。Ｓ０，０をＳ－ｂｏｘテーブル１０５により変換した結果をＳ’’０，０とする（図３

Ｓ３０４）。Ｓ’’０，０を係数テーブル１０６の第０行の４個の出力と乗算し、連結して出力する（図３Ｓ３０５）。４バイト長のガロア体乗算器１０７の出力は、累算レジスタ１１０の内容に加算される（図３Ｓ３０６）。

【００８１】

同様に、第１列第１行Ｓ１，１，第２列第２行Ｓ２，２，第３列第３行Ｓ３，３も順次処理する。列マルチプレクサ１０２は、入力ステート１０１から、それぞれ、第１，２，３列を選択、出力する。その中から、行マルチプレクサ１０４は、それぞれ、第１行のＳ１，１，第２行のＳ２，２，第３行のＳ３，３を選択、出力する。Ｓ１，１，Ｓ２，２，Ｓ３，３をそれぞれＳ－ｂｏｘテーブル１０５により変換した結果をＳ’’１，１，Ｓ’’２，２，Ｓ’’３，３とし、それぞれ係数テーブル１０６の第１，２，３行の４個の出力と乗算し、連結して出力する。４バイト長のガロア体乗算器１０７の出力は、累算レジスタ１１０の内容にガロア体加算機１０９により加算される。ガロア体乗算器１０７からの第３行の出力を累算レジスタ１１０に加算し終わると、累算レジスタ１１０に、１列４要素分のＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ結果が得られる（図３Ｓ３０７）。この得られた結果は、図２５示す非特許文献５の方法（Ｇｌａｄｍａｎの方法）の結果に等しい。

【００８２】

本発明の第１の実施の形態の特長は、図２５に示した非特許文献５（Ｇｌａｄｍａｎ）の方法における拡張Ｓ－ｂｏｘ１７０１と同等の出力を得るために必要なハードウェア量を約１／１６に削減した点にある。図２５に示した方法では、３２ビット２５６語のテーブルを４種類、計３２ｋビットのハードウェア資源が必要である。一方、図１に示した本発明の方法では、８ビット２５６語の１個のＳ－ｂｏｘテーブル１０５（計２ｋビット）とガロア体乗算器１０７とで同等の出力が得られる。

【００８３】

８ビット２５６語のＳ－ｂｏｘテーブル１０５の規模は数千～１万ゲートあり、これと比較して１個あたり数十ゲート規模でしかないガロア体乗算器１０７のコストは無視できるため、必要なハードウェア量はＳ－ｂｏｘテーブル１０５の

容量に比例するとしてよい。したがって、２ｋビットのＳ－ｂｏｘテーブル１０５を使う本発明の第１の実施の形態は、３２ｋビットのテーブルを使う非特許文献５（Ｇｌａｄｍａｎ）の方法に比べ、１／１６のハードウェア規模で同等の演算が行える効率の良い方法といえる。

【００８４】

以上、本発明の第１の実施の形態によれば、ＡＥＳ暗号化に必要なハードウェア量を大幅に削減できることを示した。その理由は、本発明の第１の実施の形態では、拡張Ｓ－ｂｏｘ１７０１の内容を全て予め計算しておく非特許文献５（Ｇｌａｄｍａｎ）の方法とは異なり、小さなＳ－ｂｏｘテーブル１０５と小規模な演算器群とを組み合わせ実行時に値を生成しているからである。

【００８５】

次に、本発明の第２の実施の形態について図面を参照して詳細に説明する。

【００８６】

図４は、本発明の第２の実施の形態の構成を示すブロック図である。

【００８７】

図５は、ＡＥＳ暗号化専用命令のニーモニック表記例を示す説明図である。

【００８８】

図６は、入力レジスタｒｓ、出力レジスタｒｔのデータ配置を示す説明図である。

【００８９】

図７は、ＡＥＳ暗号化命令の即値と出力との関係を示す説明図である。

【００９０】

本発明は、非特許文献５（Ｇｌａｄｍａｎ）のソフトウェア向けアルゴリズムと同等のシグナルフローを実現しているので、マイクロプロセッサのＡＥＳ暗号化専用命令により本発明を利用してＡＥＳ暗号の符号化、復号化の実行させることができる。本発明の第２の実施の形態は、マイクロプロセッサにＡＥＳ暗号化専用命令を追加し、図１に示した本発明の第１の実施の形態を演算器として利用し、ＡＥＳ暗号化処理を実施するものである。

【００９１】

図５に示すように、ＡＥＳ暗号化命令の名称は説明文中で参照する都合上、たとえば、“ＡＥＳ＿ＳＳＭ（ＡＥＳＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ）”とする。この命令は入力レジスタｒｓ，出力レジスタｒｔ，即値ｉｍｍの３個のオペランドをとる。入力レジスタｒｓ、出力レジスタｒｔとも、３２ビット長以上あり、ステートの要素を１列分４個連結して格納できるものとする。

【００９２】

それぞれ、図６（ａ）は、入力レジスタｒｓのデータ配置を、図６（ｂ）は、出力レジスタｒｔのデータ配置を示す。図５に示す“ＡＥＳ＿ＳＳＭ”命令は、入力レジスタｒｓの即値ｉｍｍによって指定された行の１バイトをＳ－ｂｏｘテーブル１０５で変換し（Ｓ－ｂｏｘ（）と表記）、ガロア体乗算器１０７によるＧＦ（２８）上の乗算により｛０１｝，｛０２｝，または，｛０３｝倍し、図７に示す順序で連結して出力レジスタｒｔに格納する。

【００９３】

図４を参照すると、本発明の第２の実施の形態は、レジスタファイル等で構成されるソフトウェア可視の汎用レジスタｒ０～汎用レジスタｒｎ（“ＡＥＳ＿ＳＳＭ”命令のｒｓ、ｒｔによりｒ０～ｒｎから、入力レジスタｒｓ、出力レジスタｒｔが１つずつ指定される）を含む汎用レジスタ群４０１と、“ＡＥＳ＿ＳＳＭ”命令コード等が格納される命令バッファ４０２と、デコーダ４０３と、補助レジスタ４０４と、補助レジスタ４０５と、補助レジスタ４０６と、補助レジスタ４０７と、補助レジスタ４０８と、補助レジスタ４０９と、ＸＯＲの演算が可能な汎用演算回路４１０と、演算結果レジスタ４１１と、書き込みマルチプレクサ４１２と、行マルチプレクサ１０４と、Ｓ－ｂｏｘテーブル１０５と、係数テーブル１０６と、ガロア体乗算器１０７と、演算結果レジスタ１０８とから構成される。

【００９４】

点線で囲まれた部分が、図１のＡＥＳ暗号回路１１１にほぼ相当する。補助レジスタ４０４、補助レジスタ４０５、補助レジスタ４０６、補助レジスタ４０７、補助レジスタ４０８、補助レジスタ４０９、演算結果レジスタ４１１、演算結

果レジスタ１０８は、パイプライン制御のために設けたものであり、必ずしも必要ない。

【００９５】

それぞれ３２ビットであり、入力ステート１０１の１列、ＡＥＳ暗号化命令の結果が格納される。また、汎用レジスタｒ０～汎用レジスタｒｎは、入力レジスタｒｓ、出力レジスタｒｔに割り当てられる。

【００９６】

次に、本発明の実施の第２の形態の動作について図面を参照して説明する。

【００９７】

図４を参照すると、命令バッファ４０２に格納されたＡＥＳ暗号化命令がデコーダ４０３でデコードされ、ｒｓにより、汎用レジスタ群４０１から処理される列の格納されている入力レジスタｒｓの１列４バイトのデータが選択され行マルチプレクサ１０４に入力される。行マルチプレクサ１０４では、デコーダ４０３からのｉｍｍ（行指定）にしたがって１列４バイトから１バイトのデータが選択され、補助レジスタ４０４に格納される。また、ｉｍｍは、補助レジスタ４０５に格納される。

【００９８】

Ｓ－ｂｏｘテーブル１０５では、補助レジスタ４０４からの１バイトのデータにしたがい１バイトのデータが出力され、補助レジスタ４０７に格納される。係数テーブル１０６では、補助レジスタ４０５からの行指定にしたがい図２に示す２ビット×４ビット、合計８ビットの係数が出力され、補助レジスタ４０６に格納される。

【００９９】

ガロア体乗算器１０７では、補助レジスタ４０７からの１バイトのデータと補助レジスタ４０６からの係数との乗算が実行され、８ビット×４の乗算結果が演算結果レジスタ１０８に格納される。演算結果レジスタ１０８内の８ビット×４の乗算結果は、書き込みマルチプレクサ４１２で選択され、デコーダ４０３からのｒｔにしたがい汎用レジスタ群４０１の出力レジスタｒｔに格納される。

【０１００】

図８は、ＡＥＳ＿ＳＳＭ命令を用い、ＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓを実現する命令列を示す説明図である。

【０１０１】

ここで、入力ステート１０１は、事前に、汎用レジスタ群４０１の汎用レジスタに１列ずつ格納されているとする。すなわち、レジスタｒ３にＳ３，３，Ｓ２，３，Ｓ１，３，Ｓ０，３が、レジスタｒ２にＳ３，２，Ｓ２，２，Ｓ１，２，Ｓ０，２が、レジスタｒ１にＳ３，１，Ｓ２，１，Ｓ１，１，Ｓ０，１が、レジスタｒ０にＳ３，０，Ｓ２，０，Ｓ１，０，Ｓ０，０が、この順に上位バイトから下位バイトに向かって格納されているとする。図８において、ビットごとの排他的論理和演算命令をＸＯＲと表記する。このとき、１ラウンド１列分のＳｕｂＢｙｔｅｓ，ＳｈｉｆｔＲｏｗｓ，ＭｉｘＣｏｌｕｍｎｓ処理は、図８に示す命令列で処理できる。図１と比較すると、列マルチプレクサ１０２に対する入力ステート１０１の列の指定をその列を収めたレジスタ番号の指定に、ガロア体加算器１０９を排他的論理和演算命令に置き換えることにより、図１と同等のシグナルフローを実現している。

【０１０２】

ＡＥＳ命令と同様、排他的論理和演算命令は、命令バッファ４０２からデコーダ４０３でデコードされ、汎用レジスタ群４０１の２つの汎用レジスタからそれぞれ４バイトのデータが読み出され、補助レジスタ４０８、補助レジスタ４０９に格納される。汎用演算回路４１０で、補助レジスタ４０８と補助レジスタ４０９からのデータの排他的論理輪演算が実施され、排他的論理輪演算結果の４バイトのデータが演算結果レジスタ４１１に格納される。

【０１０３】

演算結果レジスタ４１１内の４バイトの排他的論理輪演算結果は、書き込みマルチプレクサ４１２で選択され、デコーダ４０３から出力にしたがい汎用レジスタ群４０１の１つの出力レジスタｒｔに格納される。

【０１０４】

図５に示したＡＥＳ専用命令を導入すれば、ＡＥＳ暗号化処理は、１ラウンド１列あたり、図８に示した７命令で処理できる。すなわち、入力ステート１０１

全体（４列）を処理しても１ラウンドあたり２８命令で済む。たとえば１２８ビット鍵時に必要な全１０ラウンド分の処理を、これまで説明を省いたＡｄｄＲｏｕｎｄＫｅｙ１４０７を含めて行っても計３００命令程度で済む。従来の非特許文献５（Ｇｌａｄｍａｎの方法）と比較すると、本発明の第２の実施の形態によれば、Ｓ－ｂｏｘテーブル１０５の容量を１／１６と削減しながら、同等の処理速度が達成できる。

【０１０５】

次に、本発明の第３の実施の形態について図面を参照して詳細に説明する。

【０１０６】

図９は、本発明の第３の実施の形態で使用する係数テーブル１０６の内容を示す説明図である。

【０１０７】

図１０は、ＡＥＳ複号化命令の即値と出力との関係を示す説明図である。

【０１０８】

図１７は、ＩｎｖｅｒｓｅＳ－ｂｏｘの内容を示す説明図である。

【０１０９】

本発明の第３の実施の形態は、ＡＥＳ復号化に関するものである。これらは、図１～図８で説明したＡＥＳ暗号化処理装置、およびＡＥＳ暗号化命令と同様に構成できる。

【０１１０】

ＡＥＳ復号化装置は、図１の係数テーブル１０６の内容を、非特許文献１（ＦＩＰＳ１９７，式（５．１０））の係数行列を転置したもの（図９）に変更し、Ｓ－ｂｏｘテーブル１０５の内容を非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ１４）に示されたＩｎｖｅｒｓｅＳ－ｂｏｘに変更したもの（図１７）である。この変更にともない、ＡＥＳ暗号化装置では係数テーブル１０６の出力が２ビット×４組であったのに対し、ＡＥＳ復号化装置では係数テーブル１０６の出力が４ビット×４組になるので、ガロア体乗算器１０７の各部分乗算器は、８×４ビット構成とする必要もある。

【０１１１】

ＡＥＳ復号化命令は、図４のうち係数テーブル１０６の内容を図９に示した非特許文献１（ＦＩＰＳ１９７，式（５．１０））の係数行列を転置したものに変更し、Ｓ－ｂｏｘの内容を非特許文献１（ＦＩＰＳ１９７，Ｆｉｇｕｒｅ１４）に示されたＩｎｖｅｒｓｅＳ－ｂｏｘに変更したものである。この変更にともない、係数テーブル１０６の出力が４ビット×４組になるので、ガロア体乗算器１０７を各８×４ビット構成とする必要もある。ＡＥＳ復号化命令の入出力関係を図１０に示す。ここでＩｎｖＳ－ｂｏｘ（）はＩｎｖｅｒｓｅＳ－ｂｏｘテーブルによる換字を表す。

【０１１２】

次に、本発明の第４の実施の形態について図面を参照して詳細に説明する。

【０１１３】

図１１は、本発明の第４の実施の形態の構成を示すブロック図である。

【０１１４】

ＡＥＳ暗号化装置とＡＥＳ復号化装置は、Ｓ－ｂｏｘおよび係数テーブルの内容が異なり、ガロア体乗算器１０７のビット幅が異なるだけなので、ＡＥＳ暗号化と復号化の両方が行える装置が容易に構成できる。また、ＡＥＳ暗号化と復号化の両方が行えるＡＥＳ暗号化・復号化統合命令も容易に構成できる。

【０１１５】

図１１を参照すると、本発明の第４の実施の形態は、図４に示したＡＥＳ暗号化命令のための演算器と、図９，図１０を参照して説明したＡＥＳ復号化命令のための演算器を統合し、ＡＥＳ暗号化と復号化の双方に対応させた演算器である。詳細には、逆アフィン変換回路１１０１と、暗号化マルチプレクサ１１０２と、逆数テーブル１１０３と、アフィン変換回路１１０４と、暗号化マルチプレクサ１１０５と、行マルチプレクサ１０４と、係数テーブル１０６と、ガロア体乗算器１０７と、演算結果レジスタ１０８とから構成される。

【０１１６】

図１８は、逆アフィン変換回路１１０１の内容を示す説明図である。

【０１１７】

図１８を参照すると、$0 \leqq i \leqq 7$であり、b_iは、入力バイトの第ｉビット、

Ｃｉは、｛０５｝の第ｉビットであり、ｂ’ｉは、出力の第ｉビットである。＜ＸＯＲ＞は、排他的論理和である。

【０１１８】

図１９は、逆数テーブル１１０３の内容を示す説明図である。

【０１１９】

図２０は、アフィン変換回路１１０４の内容を示す説明図である。

【０１２０】

図２０を参照すると、０≦ｉ≦７であり、ｂｉは、入力バイトの第ｉビット、Ｃｉは、｛６３｝の第ｉビットであり、ｂ’ｉは、出力の第ｉビットである。＜ＸＯＲ＞は、排他的論理和である。

【０１２１】

非特許文献１（ＦＩＰＳ１９７，５．１．１節）に記述されているように、暗号化で用いるＳ－ｂｏｘテーブル１０５は入力値のＧＦ（２８）上の逆数に、非特許文献１（ＦＩＰＳ１９７，式（５．１））に示されるアフィン変換を施したものである。また、復号化で用いるＩｎｖｅｒｓｅＳ－ｂｏｘテーブルは、Ｓ－ｂｏｘテーブル１０５の逆関数なので、入力値に、非特許文献１（ＦＩＰＳ１９７，式（５．１））に示されるアフィン変換の逆変換（以下「逆アフィン変換」）を施した後、ＧＦ（２８）上の逆数をとったものである。したがって、逆数テーブル１１０３を１個用意し、暗号化時においては、逆数テーブル１１０３の出力にアフィン変換回路１１０４による変換を施してＳ－ｂｏｘテーブル１０５と同等の出力を得ることが可能であり、復号化時においては、逆数テーブル１１０３の入力に逆アフィン変換回路１１０１による変換を施してＩｎｖｅｒｓｅＳ－ｂｏｘテーブルと同等の出力を得ることが可能である。

【０１２２】

暗号化と復号化の切り替えは、命令語の即値（ｉｍｍ）を１ビット増やして指定することで行える。このビットにしたがい、暗号化マルチプレクサ１１０２、暗号化マルチプレクサ１１０５により、暗号化時は逆数テーブル１１０３の出力にアフィン変換を、復号化時は、逆数テーブル１１０３の入力に逆アフィン変換を施す。また、このビットは係数テーブル１０６の出力を、暗号化時は図２に示

した内容を、復号化時は図９に示した内容を出力するよう切り替える。

【０１２３】

以上、図１１を参照しながら、ＡＥＳ暗号化および復号化で共用できる演算器を構成するため、図１、または、図４に施した変更点を説明した。図１１に示す本発明の第4の実施の形態によれば、８ビット×２５６ワード（２ｋビット）のテーブル１個で、ＡＥＳ暗号化または復号化を４並列で処理できる。

【０１２４】

従来の技術で説明した非特許文献５（Ｇｌａｄｍａｎの方法）では、暗号化のために３２ｋビットのテーブルを用意する必要があったが、このテーブルは復号化とは共用できず、復号化用にも別に３２ｋビットのテーブルを用意する必要がある。すなわち、非特許文献５（Ｇｌａｄｍａｎの方法）により暗号化と復号化を行おうとすると、計６４ｋビットのテーブルを用意する必要がある。

【０１２５】

一方、本発明の第４の実施の形態では、同等の演算を２ｋビットのテーブルで行うため、必要なテーブル容量を１／３２まで削減できる。

【０１２６】

次に、本発明の第２～第４の実施の形態で説明したＡＥＳ暗号化・復号化命令のバリエーションについて説明する。

【０１２７】

ＡＥＳ暗号化命令では、図４において、即値が、行マルチプレクサ１０４、および、係数テーブル１０６に対し処理対象となる行番号そのものを指定するとしたが、４種類の出力を区別できるなら、図７に示した即値のビットパターンに縛られるものではない。同様の議論はＡＥＳ復号化命令、ＡＥＳ暗号化・復号化統合命令にも適用可能である。

【０１２８】

ＡＥＳ暗号化命令が演算対象とする要素のレジスタ上のバイト位置を指定するため、図４では、ＡＥＳ暗号化命令の引数に即値を与えるとしたが、その代わりに命令コードの一部を用いて選択すべき行を指定することもできる。言い換えれば、扱う行別に４種類の命令を用意し、入力レジスタ番号と出力レジスタ番号の

みを引数に与えてもよい。同様の議論は、ＡＥＳ復号化命令、ＡＥＳ暗号化・復号化統合命令にも適用可能である。

【０１２９】

図５に示したＡＥＳ暗号化命令では、ロード・ストア・アーキテクチャのマイクロプロセッサを想定したため、入出力データはレジスタファイルで構成される汎用レジスタに置き、命令の引数にレジスタ番号を指定するとしたが、演算の入出力データの片方、または、両方をメモリ上に置けるマイクロプロセッサを想定し、専用命令の引数に何らかのメモリ・アドレス指定を取るよう変更しても、本発明の第２の実施例の本質に影響を与えないため、同様の効果が得られる。同様の議論はＡＥＳ復号化命令、ＡＥＳ暗号化・復号化統合命令にも適用可能である。

【０１３０】

図８で示したように、ＡＥＳ暗号化命令の出力に対しＸＯＲ命令を発行することが多い。したがって、図４では、ＡＥＳ暗号化命令が、ガロア体乗算器１０７出力と同等の結果を生成するとしたが、累算レジスタ（図８のｒ５）も入力に取る３レジスタ命令とし、図１のガロア体加算器１０９出力と同等の結果を生成するよう変更し、高速化を図ることもできる。同様の議論はＡＥＳ復号化命令、ＡＥＳ暗号化・復号化統合命令にも適用可能である。

【０１３１】

図６に示したように、ＡＥＳ暗号化命令、ＡＥＳ復号化命令、ＡＥＳ暗号化・復号化統合命令では、現在、一般的なレジスタ幅が３２ビットのマイクロプロセッサを想定したが、レジスタ幅が３２ビットよりも広いマイクロプロセッサでも、レジスタの下位３２ビットのみ使用することで同様の命令を導入することができる。

【０１３２】

次に、本発明の第５の実施の形態について図面を参照して詳細に説明する。

【０１３３】

図１２は、本発明の第５の実施の形態の構成を示すブロック図である。

【０１３４】

本発明の第５の実施の形態では、６４ビット・レジスタを持つマイクロプロセッサに適用され、暗号化・復号化演算器を２重化し、レジスタの上位と下位で同時に演算することで、性能を約２倍にできる。

【０１３５】

図１２において、６４ビット長の入力レジスタ１２０１（汎用レジスタに割り当てられる）は、ｂｉ０～ｂｉ７までの８要素を保持する。図１１の構成をＡＥＳ処理命令向けの演算器コアとして多重化し（演算器コア１２０２，演算器コア１２０３）、上位４要素をひとつの演算器コア１２０２へ、下位４要素をもうひとつの演算器コア１２０３へ入力する。演算器コア１２０２、演算器コア１２０３の出力は連結され、６４ビット長の出力レジスタ１２０４（汎用レジスタに割り当てられる）へ格納される。

【０１３６】

係数テーブル１０６と、行、暗号化・復号化を指定する即値とは、演算器コア１２０２、演算器コア１２０３で共用できる。６４ビットより幅広のレジスタを持つマイクロプロセッサでも、同様の演算器コア多重化による性能拡張が可能である。入力レジスタ１２０１に置く複数のステートの列は、同一ステート内の異なる列でもよいし、別のステートの列でも構わない。

【０１３７】

【発明の効果】

本発明の効果は、ＡＥＳ暗号化および復号化に必要なテーブル容量を従来に比べ削減できることである。たとえば、非特許文献５（Ｇｌａｄｍａｎの方法）では、暗号化と復号化を併せると６４ｋビットのテーブルを必要としていた。

【０１３８】

本発明では、２ｋビットのテーブル１個で暗号化、復号化の双方に対応しており、必要テーブル容量を１／３２に削減できる。これはＡＥＳ専用のアクセラレータや、マイクロプロセッサに専用ＡＥＳ命令を実装するための演算器が小面積で構成できることを示している。

【０１３９】

さらに、マイクロプロセッサに本発明のＡＥＳ演算器コアを使ったＡＥＳ処理

専用命令を導入すれば外部メモリに置くＳ－ｂｏｘテーブルは不要になる。

【０１４０】

従って組み込み機器など外部メモリ容量に制限がある場合でもＡＥＳ暗号化機能を組み込めるようになるという利点がある。外部メモリ容量に強い制限のないハイエンド機器においても、メモリ上のテーブルをアクセスする替わりに、ＡＥＳ処理専用命令を使えば、キャッシュ汚染を防ぎ高速化につながるという利点がある。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態の構成を示すブロック図である。

【図２】

図１の係数テーブルの内容を示す説明図である。

【図３】

本発明の第１の実施の形態の動作を示す説明図である。

【図４】

本発明の第２の実施の形態の構成を示すブロック図である。

【図５】

ＡＥＳ暗号化専用命令のニーモニック表記例を示す説明図である。

【図６】

入力レジスタ、出力レジスタのデータ配置を示す説明図である。

【図７】

ＡＥＳ暗号化命令の即値と出力との関係を示す説明図である。

【図８】

ＡＥＳ＿ＳＳＭ命令を含む命令列を示す説明図である。

【図９】

本発明の第３の実施の形態で使用する係数テーブルの内容を示す説明図である。

【図１０】

ＡＥＳ複号化命令の即値と出力との関係を示す説明図である。

【図１１】

本発明の第４の実施の形態の構成を示すブロック図である。

【図１２】

本発明の第５の実施の形態の構成を示すブロック図である。

【図１３】

ＧＦ（２８）上の加算器の例を示すブロック図である。

【図１４】

ＧＦ（２８）上の２倍回路の例を示すブロック図である。

【図１５】

ＧＦ（２８）上のガロア体乗算器の例を示すブロック図である。

【図１６】

図１のＳ－ｂｏｘテーブルの内容を示す説明図である。

【図１７】

ＩｎｖｅｒｓｅＳ－ｂｏｘの内容を示す説明図である。

【図１８】

逆アフィン変換回路の内容を示す説明図である。

【図１９】

逆数テーブルの内容を示す説明図である。

【図２０】

アフィン変換回路の内容を示す説明図である。

【図２１】

ＡＥＳ暗号のデータ構造であるステートを示す説明図である。

【図２２】

ＡＥＳ暗号化の手順を示すフローチャートである。

【図２３】

ＡＥＳ暗号化のラウンド処理の一部を示すシグナルフローである。

【図２４】

従来の非特許文献４（ＭｃＬｏｏｎｅら）の高速化手法を示すシグナルフローである。

【図２５】

非特許文献５の高速化手法を示すシグナルフローである。

【図２６】

ＡＥＳ復号化の手順を示すフローチャートである。

【符号の説明】

１０１　入力ステート

１０２　列マルチプレクサ

１０３　演算入力レジスタ

１０４　行マルチプレクサ

１０５　Ｓ－ｂｏｘテーブル

１０６　係数テーブル

１０７　ガロア体乗算器

１０８　演算結果レジスタ

１０９　ガロア体加算器

１１０　累算レジスタ

１１１　ＡＥＳ暗号回路

４０１　汎用レジスタ群

４０２　命令バッファ

４０３　デコーダ

４０４　補助レジスタ

４０５　補助レジスタ

４０６　補助レジスタ

４０７　補助レジスタ

４０８　補助レジスタ

４０９　補助レジスタ

４１０　汎用演算回路

４１１　演算結果レジスタ

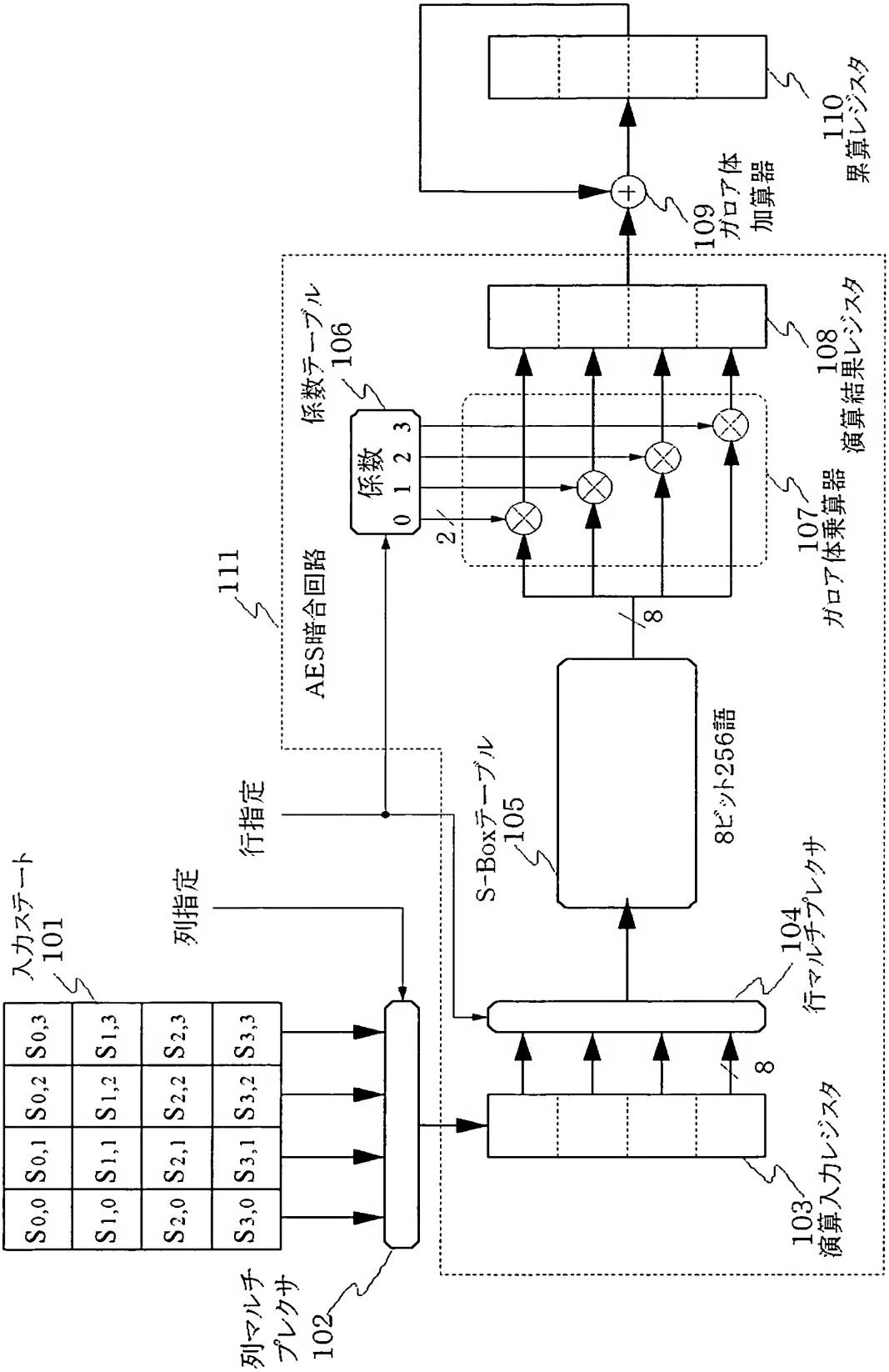
４１２　書き込みマルチプレクサ

１１０１　逆アフィン変換回路

１１０２　暗号化マルチプレクサ
１１０３　逆数テーブル
１１０４　アフィン変換回路
１１０５　暗号化マルチプレクサ
１２０１　入力レジスタ
１２０２　演算器コア
１２０３　演算器コア
１２０４　出力レジスタ

【書類名】　図面

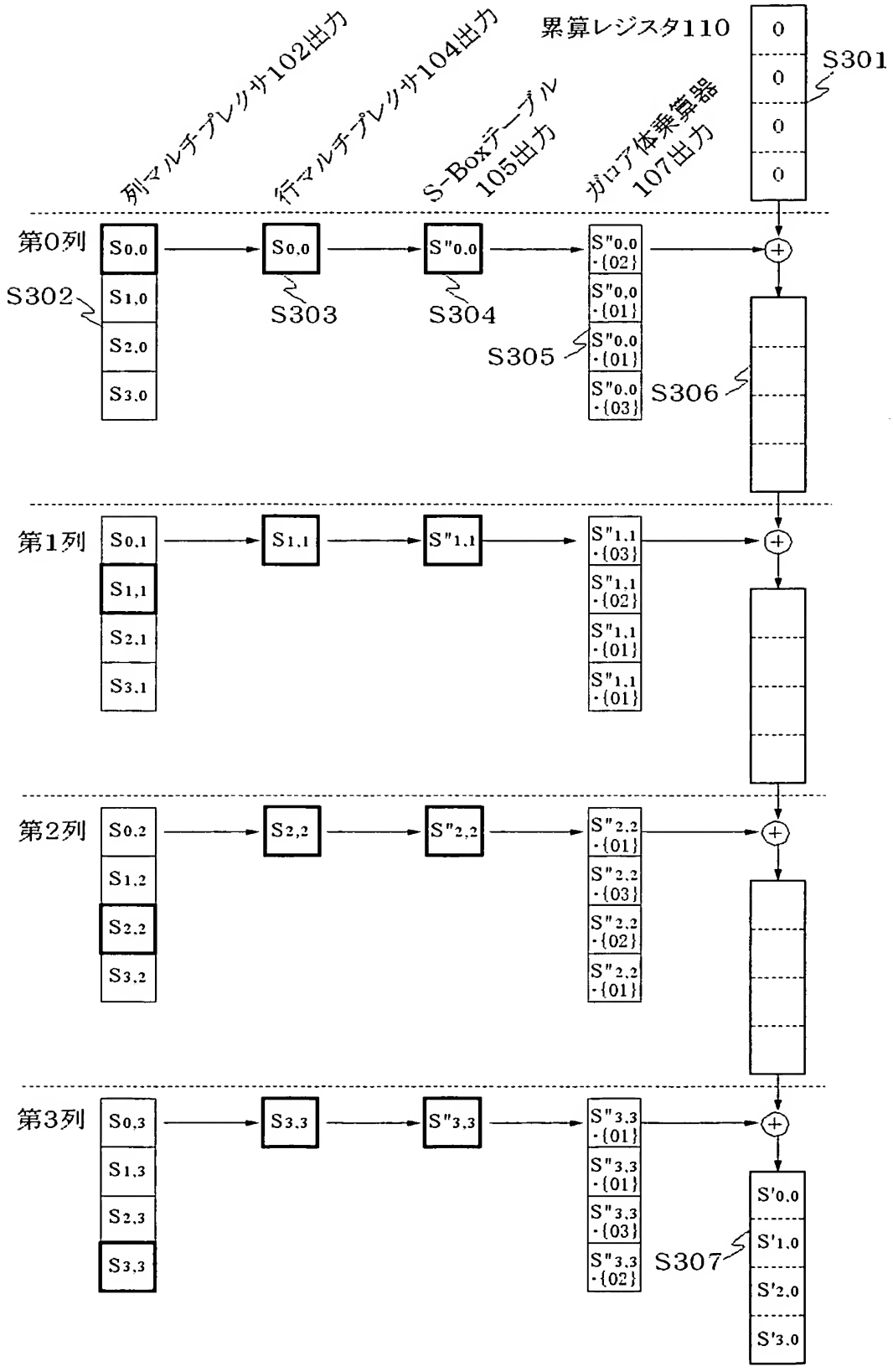
【図１】


入力ステート
101
S0,0 S0,1 S0,2 S0,3
S1,0 S1,1 S1,2 S1,3
S2,0 S2,1 S2,2 S2,3
S3,0 S3,1 S3,2 S3,3
列指定
行指定
列マルチプレクサ
102
AES暗合回路
111
係数テーブル
106
係数
0 1 2 3
2
S-Boxテーブル
105
8ビット256語
8
8
演算入力レジスタ
103
行マルチプレクサ
104
ガロア体乗算器
107
演算結果レジスタ
108
ガロア体
加算器
109
累算レジスタ
110

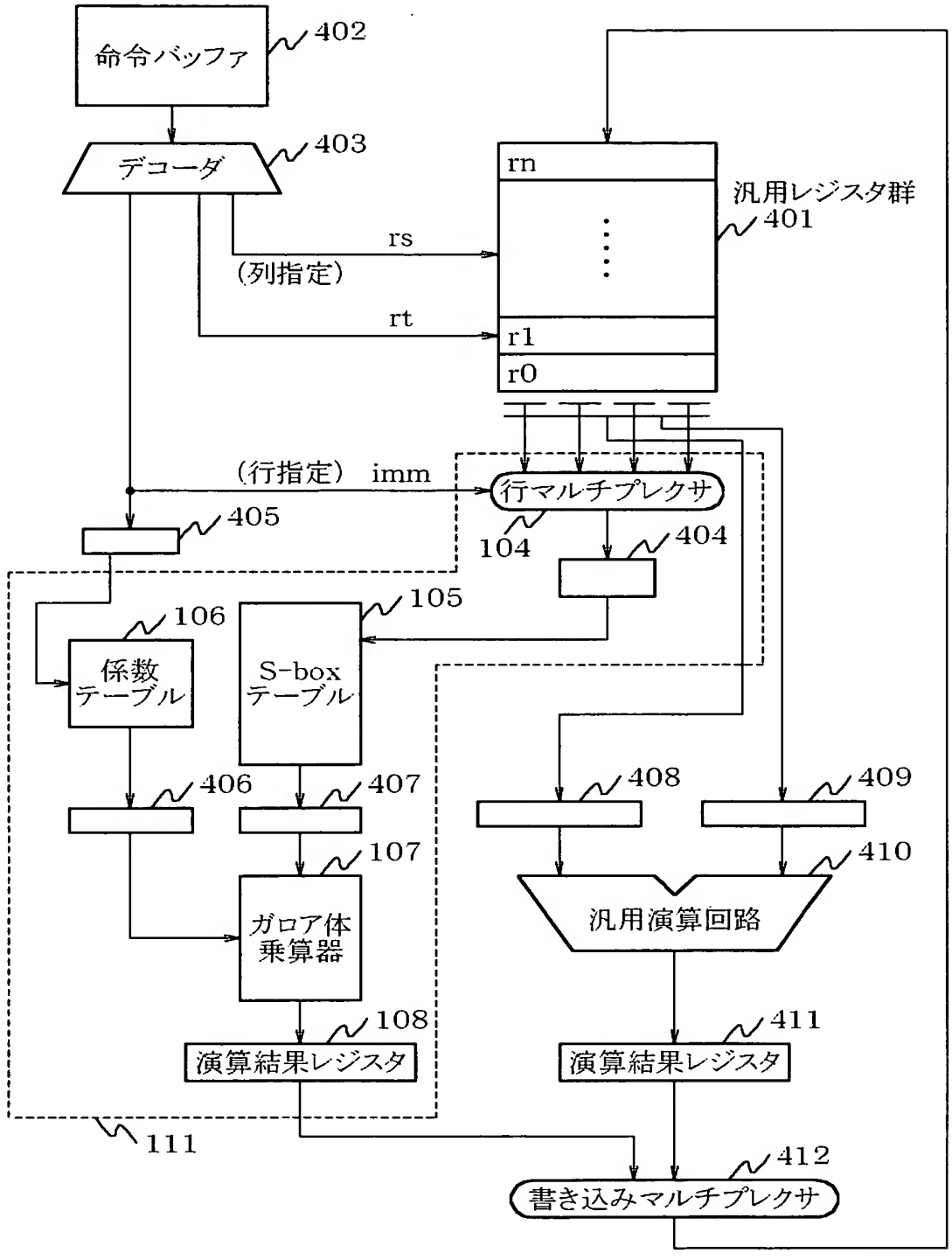
【図２】

行指定	係数テーブル出力			
	係数3	係数2	係数1	係数0
0	{02}	{01}	{01}	{03}
1	{03}	{02}	{01}	{01}
2	{01}	{03}	{02}	{01}
3	{01}	{01}	{03}	{02}

【図３】


列マルチプレクサ102出力
行マルチプレクサ104出力
S-Boxテーブル 105出力
ガロア体乗算器 107出力
累算レジスタ110
0
0
0
0
S301
第0列
S0,0
S1,0
S2,0
S3,0
S302
S0,0
S303
S"0,0
S304
S"0,0 ·{02}
S"0,0 ·{01}
S"0,0 ·{01}
S"0,0 ·{03}
S305
S306
第1列
S0,1
S1,1
S2,1
S3,1
S1,1
S"1,1
S"1,1 ·{03}
S"1,1 ·{02}
S"1,1 ·{01}
S"1,1 ·{01}
第2列
S0,2
S1,2
S2,2
S3,2
S2,2
S"2,2
S"2,2 ·{01}
S"2,2 ·{03}
S"2,2 ·{02}
S"2,2 ·{01}
第3列
S0,3
S1,3
S2,3
S3,3
S3,3
S"3,3
S"3,3 ·{01}
S"3,3 ·{01}
S"3,3 ·{03}
S"3,3 ·{02}
S307
S'0,0
S'1,0
S'2,0
S'3,0

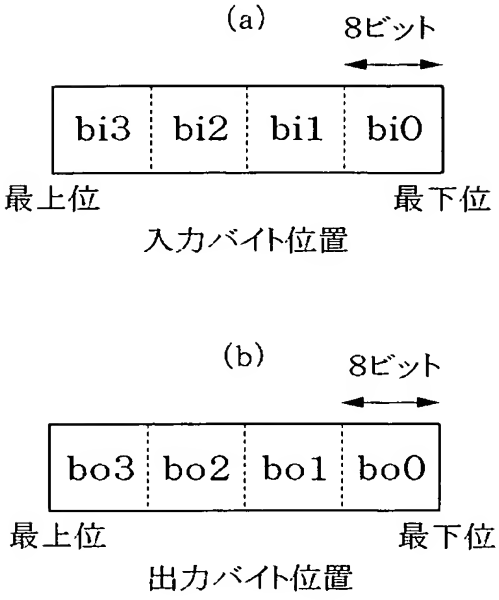
【図４】


命令バッファ
402
デコーダ
403
rn
汎用レジスタ群
401
rs
(列指定)
rt
r1
r0
(行指定)　imm
行マルチプレクサ
104
405
404
106
係数
テーブル
105
S-box
テーブル
406
407
408
409
107
410
ガロア体
乗算器
汎用演算回路
108
411
演算結果レジスタ
演算結果レジスタ
111
412
書き込みマルチプレクサ

【図５】

AES_SSM rs, rt, imm
rs：入力レジスタ
rt：出力レジスタ
imm：即値

【図６】



【図７】

入力即値	出力			
行指定	bo3	bo2	bo1	bo0
00	S-box(bi0)・{02}	S-box(bi0)・{01}	S-box(bi0)・{01}	S-box(bi0)・{03}
01	S-box(bi1)・{03}	S-box(bi1)・{02}	S-box(bi1)・{01}	S-box(bi1)・{01}
02	S-box(bi2)・{01}	S-box(bi2)・{03}	S-box(bi2)・{02}	S-box(bi2)・{01}
03	S-box(bi3)・{01}	S-box(bi3)・{01}	S-box(bi3)・{03}	S-box(bi3)・{02}

【図８】

```
; 入力:
; r0=[S3,0 S2,0 S1,0 S0,0]
; r1=[S3,1 S2,1 S1,1 S0,1]
; r2=[S3,2 S2,2 S1,2 S0,2]
; r3=[S3,3 S2,3 S1,3 S0,3]
;
; 作業用レジスタ:r4
; 累算レジスタ:r5
;
; 出力:
; r5=[S'3,0  S'2,0  S'1,0  S'0,0 ]
;
AES_SSM r0, r5, 0  ; S0,0= r0, bi0
AES_SSM r1, r4, 1  ; S1,1= r1, bi1
XOR     r5, r4, r5 ; r5 = r5 XOR r4
AES_SSM r2, r4, 2  ; S2,2= r2, bi2
XOR     r5, r4, r5 ; r5 = r5 XOR r4
AES_SSM r3, r4, 3  ; S3,3= r3, bi3
XOR     r5, r4, r5 ; r5 = r5 XOR r4
```

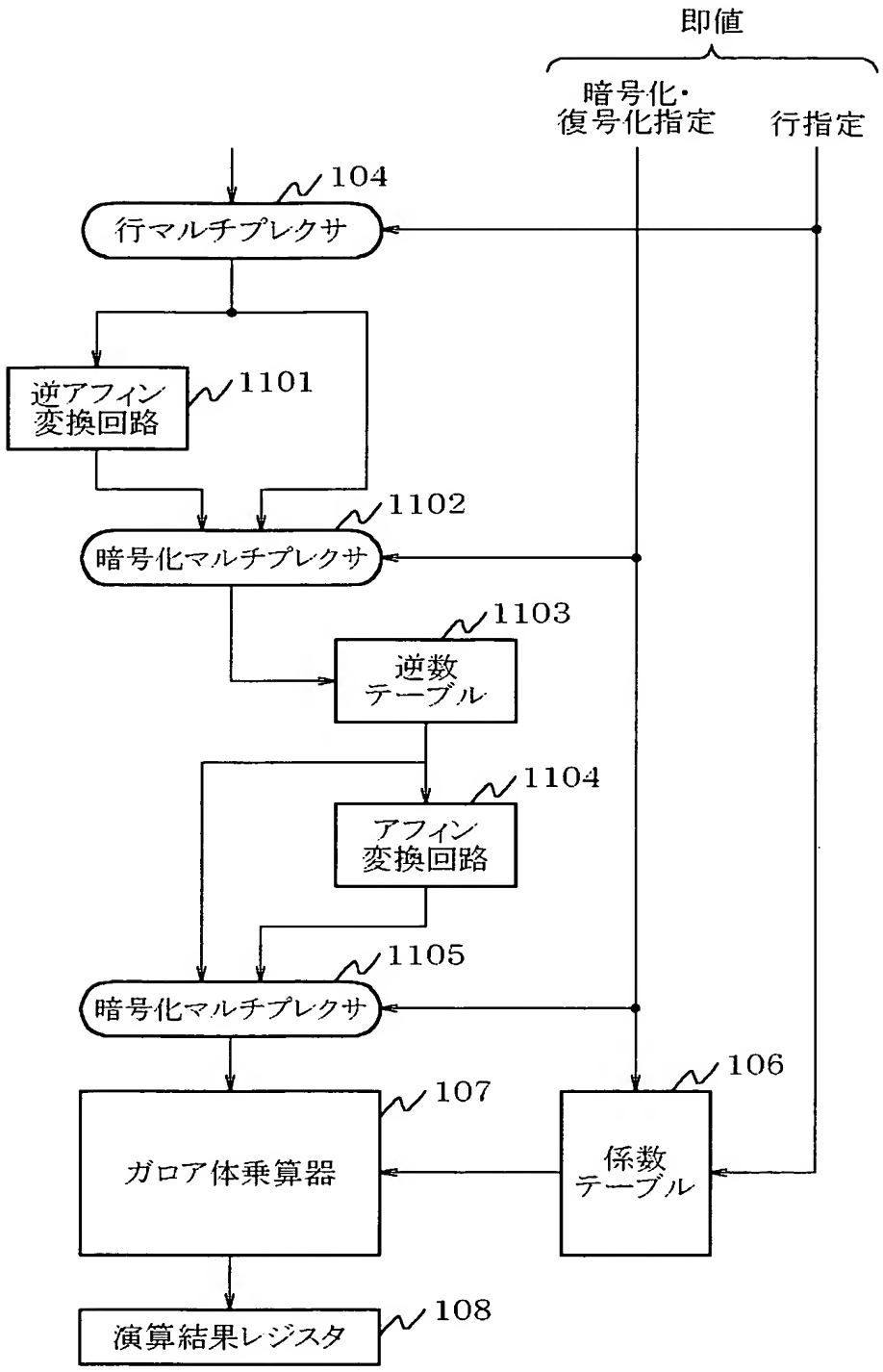
【図９】

行指定	係数テーブル出力			
	係数3	係数2	係数1	係数0
0	{0e}	{09}	{0d}	{0b}
1	{0b}	{0e}	{09}	{0d}
2	{0d}	{0b}	{0e}	{09}
3	{09}	{0d}	{0b}	{0e}

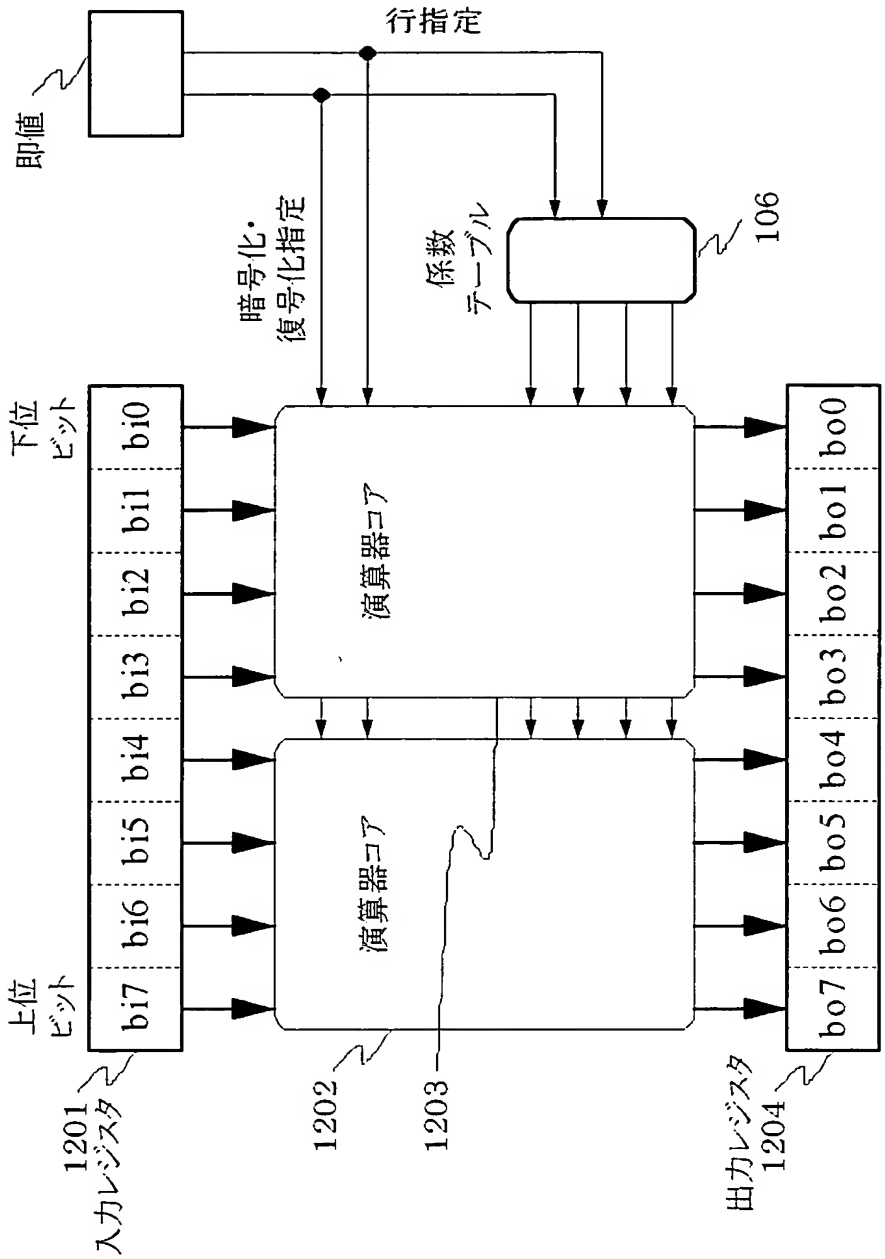
【図１０】

入力即値	出力			
行指定	bo3	bo2	bo1	bo0
00	InvS-box(bi0)・{0e}	InvS-box(bi0)・{09}	InvS-box(bi0)・{0d}	InvS-box(bi0)・{0b}
01	InvS-box(bi1)・{0b}	InvS-box(bi1)・{0e}	InvS-box(bi1)・{09}	InvS-box(bi1)・{0d}
02	InvS-box(bi2)・{0d}	InvS-box(bi2)・{0b}	InvS-box(bi2)・{0e}	InvS-box(bi2)・{09}
03	InvS-box(bi3)・{09}	InvS-box(bi3)・{0d}	InvS-box(bi3)・{0b}	InvS-box(bi3)・{0e}

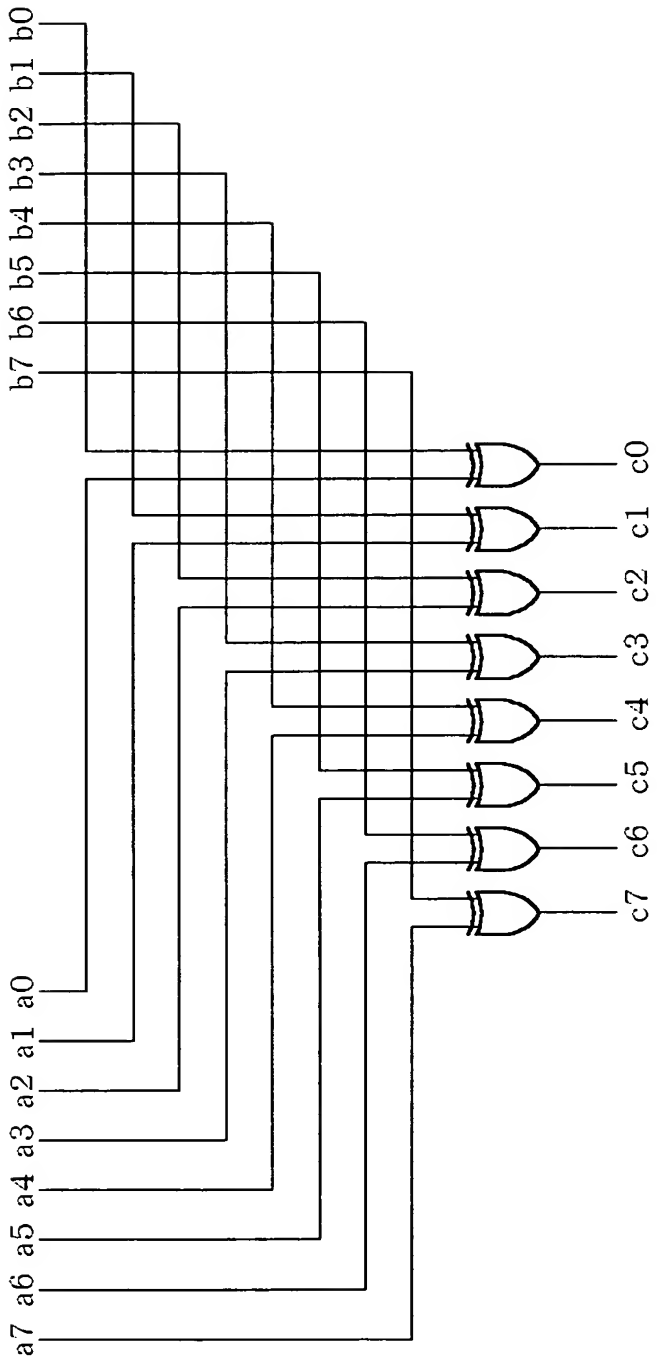
【図１１】


即値
暗号化・
復号化指定
行指定
104
行マルチプレクサ
逆アフィン
変換回路
1101
1102
暗号化マルチプレクサ
1103
逆数
テーブル
1104
アフィン
変換回路
1105
暗号化マルチプレクサ
106
107
ガロア体乗算器
係数
テーブル
108
演算結果レジスタ

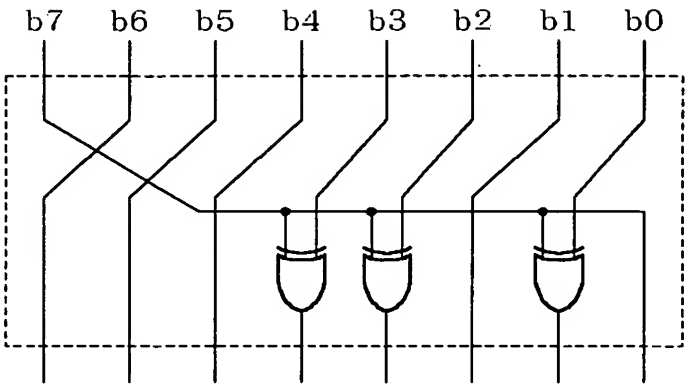
【図１２】


即値
行指定
暗号化・
復号化指定
係数
テーブル
106
下位
ビット
bi0
bi1
bi2
bi3
bi4
bi5
bi6
bi7
上位
ビット
演算器コア
演算器コア
bo0
bo1
bo2
bo3
bo4
bo5
bo6
bo7
1201
入力レジスタ
1202
1203
出力レジスタ
1204

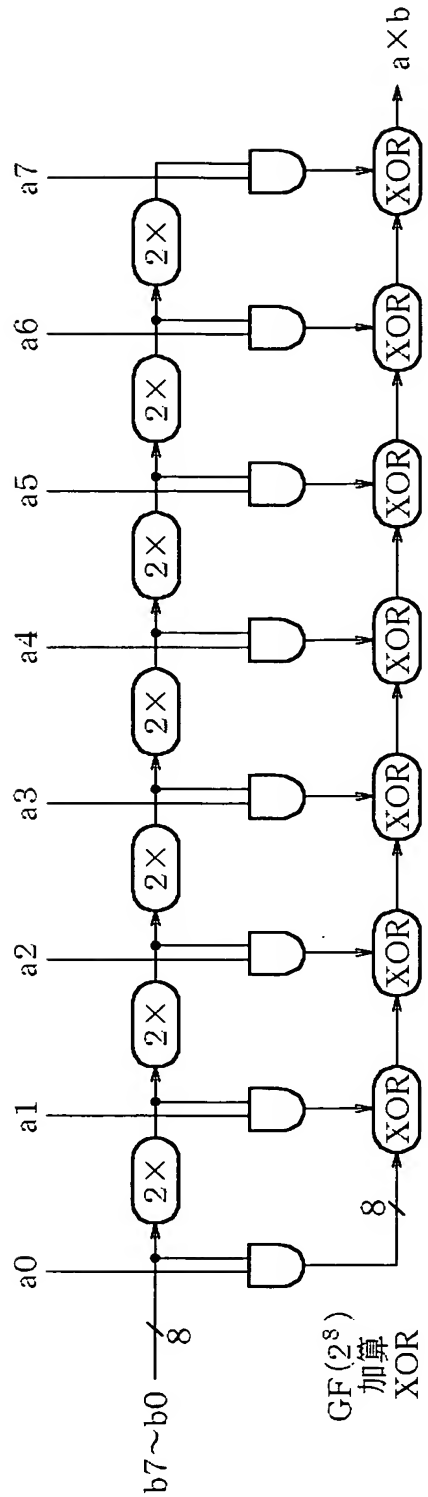
【図１３】



【図１４】



【図１５】



【図１６】

下位

上位 x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

【図１７】

下位

上位 x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

【図１８】

$$b'_i = b_{(i+2) \bmod 8} \langle XOR \rangle b_{(i+5) \bmod 8} \langle XOR \rangle b_{(i+7) \bmod 8} \langle XOR \rangle c_i$$

【図１９】

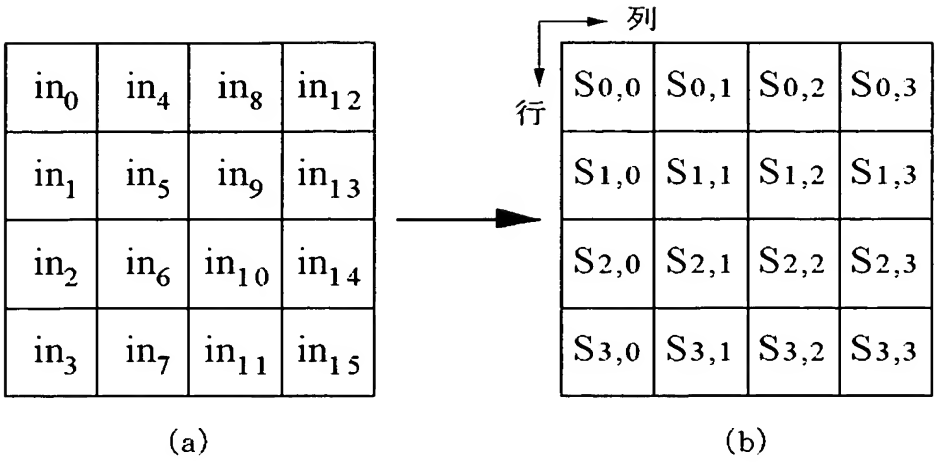
下位

上位 x	y 0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19
4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b
7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4
9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a
a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62
b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57
c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6
d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b
e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	e3	5d	50	1e	b3
f	5b	23	38	34	68	46	03	8c	dd	9c	7d	a0	cd	1a	41	1c

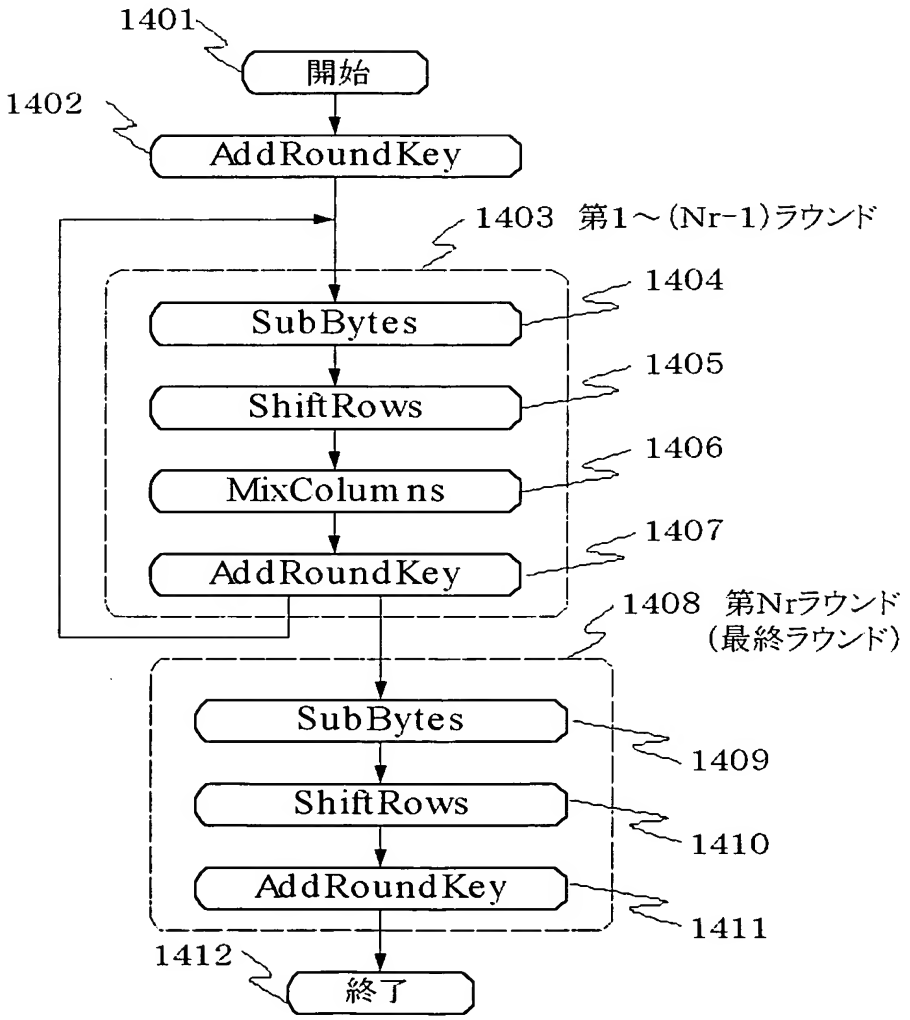
【図２０】

$$b'_i = b_i \langle XOR \rangle b_{(i+4) \bmod 8} \langle XOR \rangle b_{(i+5) \bmod 8} \langle XOR \rangle b_{(i+6) \bmod 8} \langle XOR \rangle b_{(i+7) \bmod 8} \langle XOR \rangle c_i$$

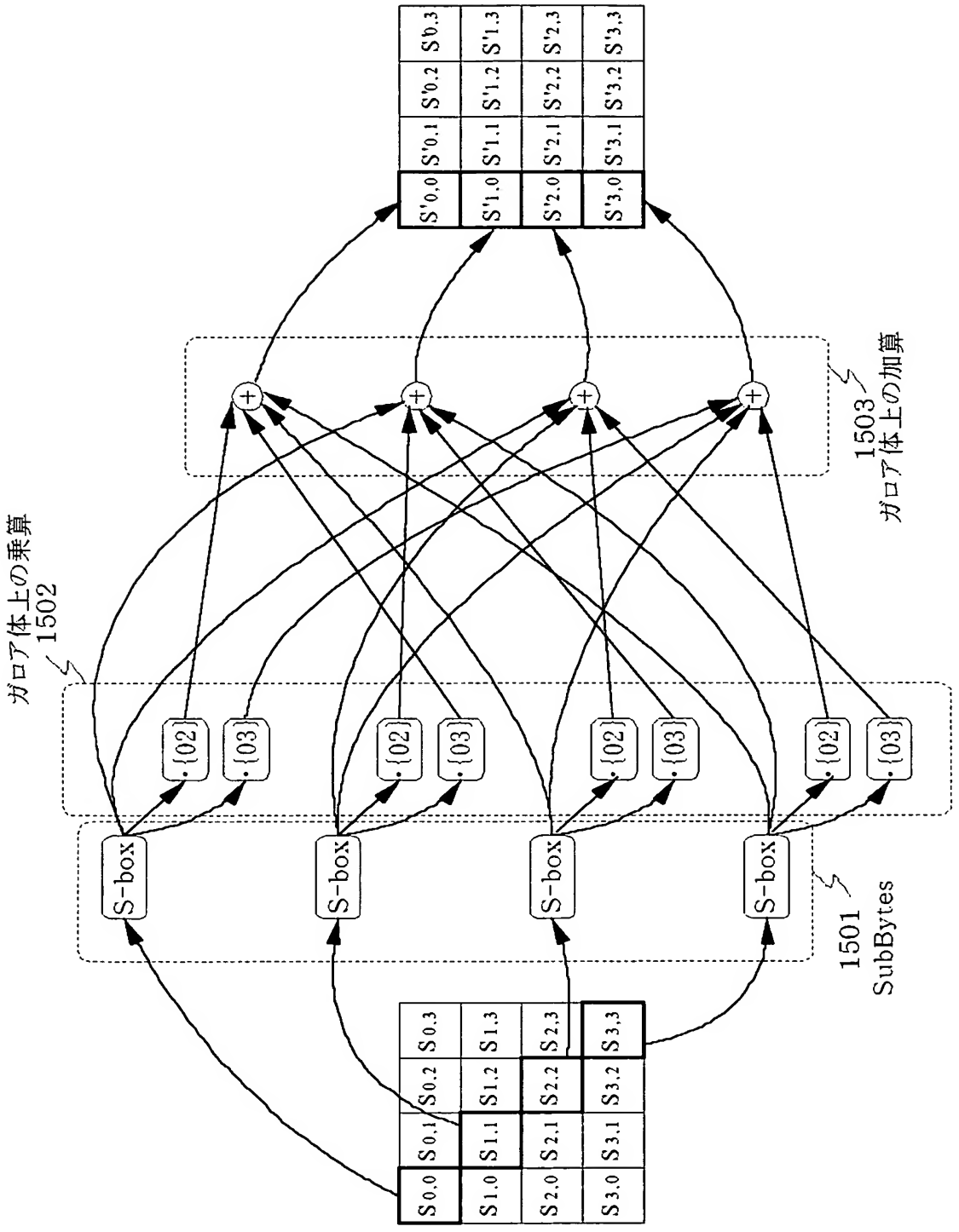
【図２１】


列
行
in0 in4 in8 in12
in1 in5 in9 in13
in2 in6 in10 in14
in3 in7 in11 in15
S0,0 S0,1 S0,2 S0,3
S1,0 S1,1 S1,2 S1,3
S2,0 S2,1 S2,2 S2,3
S3,0 S3,1 S3,2 S3,3
(a)
(b)

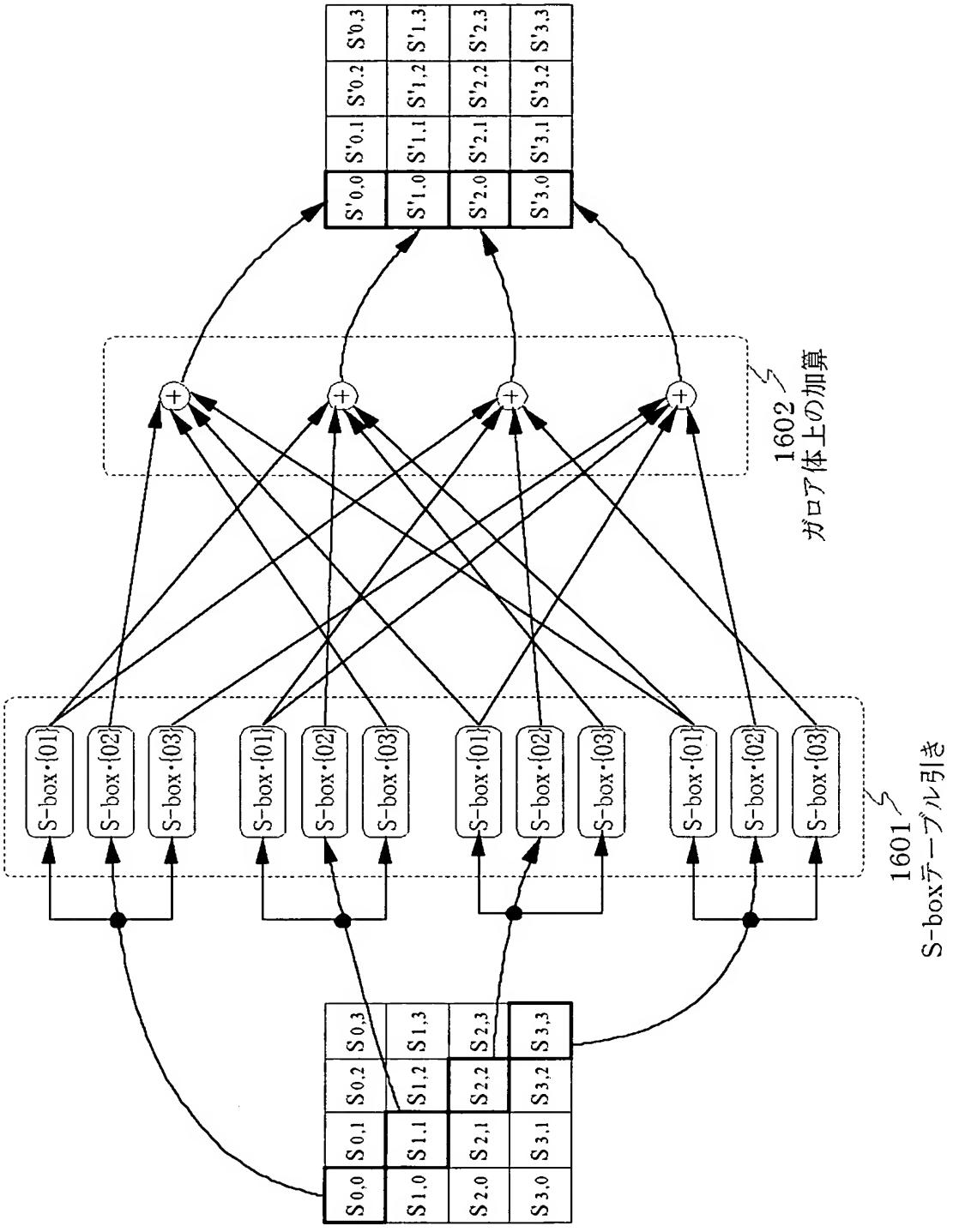
【図２２】


1401
開始
1402
AddRoundKey
1403 第1～(Nr-1)ラウンド
1404
SubBytes
1405
ShiftRows
1406
MixColumns
1407
AddRoundKey
1408 第Nrラウンド
(最終ラウンド)
SubBytes
1409
ShiftRows
1410
AddRoundKey
1411
1412
終了

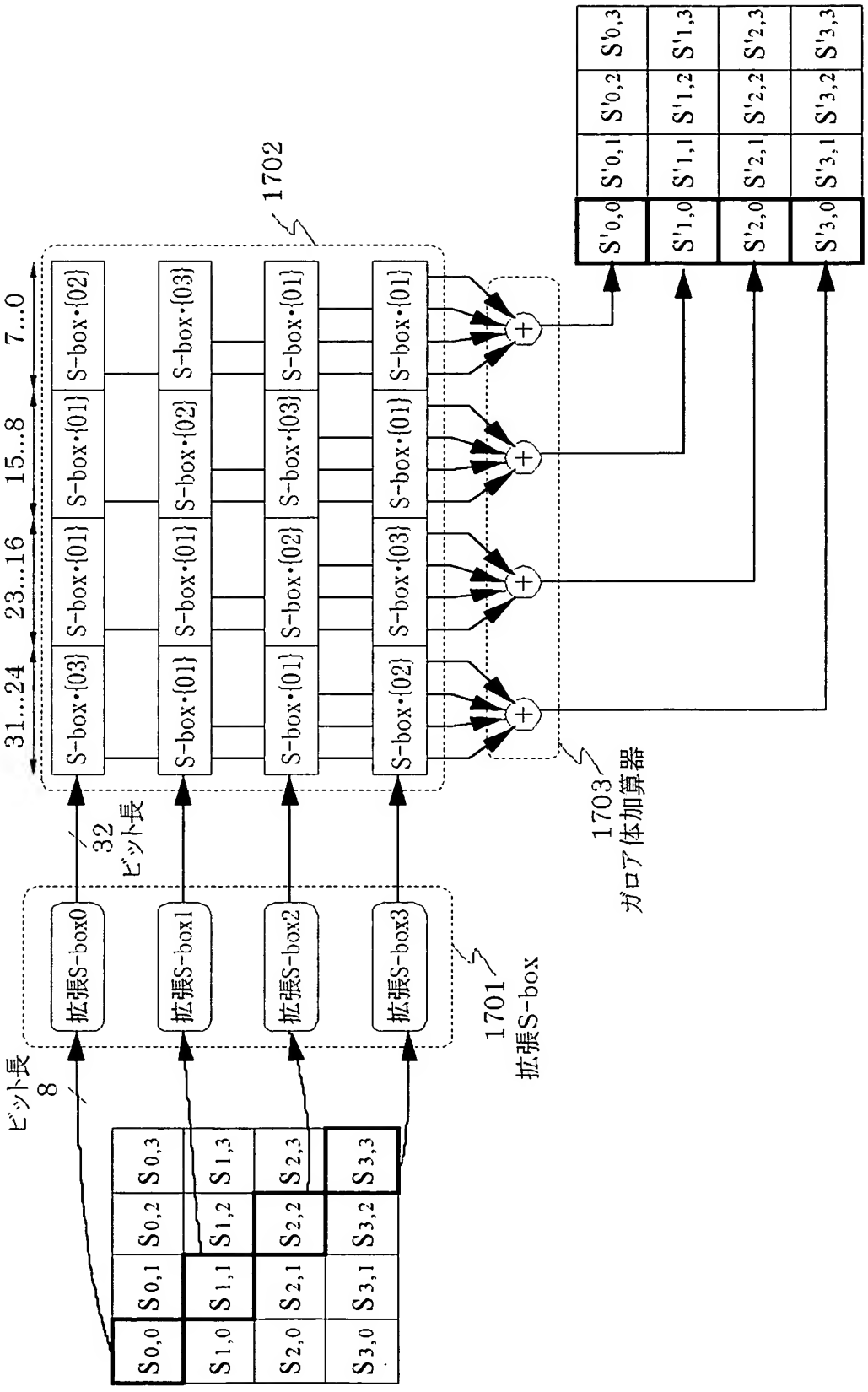
【図２３】


S'0,0 S'1,0 S'2,0 S'3,0
S'0,1 S'1,1 S'2,1 S'3,1
S'0,2 S'1,2 S'2,2 S'3,2
S'0,3 S'1,3 S'2,3 S'3,3
ガロア体上の加算
1503
ガロア体上の乗算
1502
{02}
{03}
S-box
SubBytes
1501
S0,0 S1,0 S2,0 S3,0
S0,1 S1,1 S2,1 S3,1
S0,2 S1,2 S2,2 S3,2
S0,3 S1,3 S2,3 S3,3

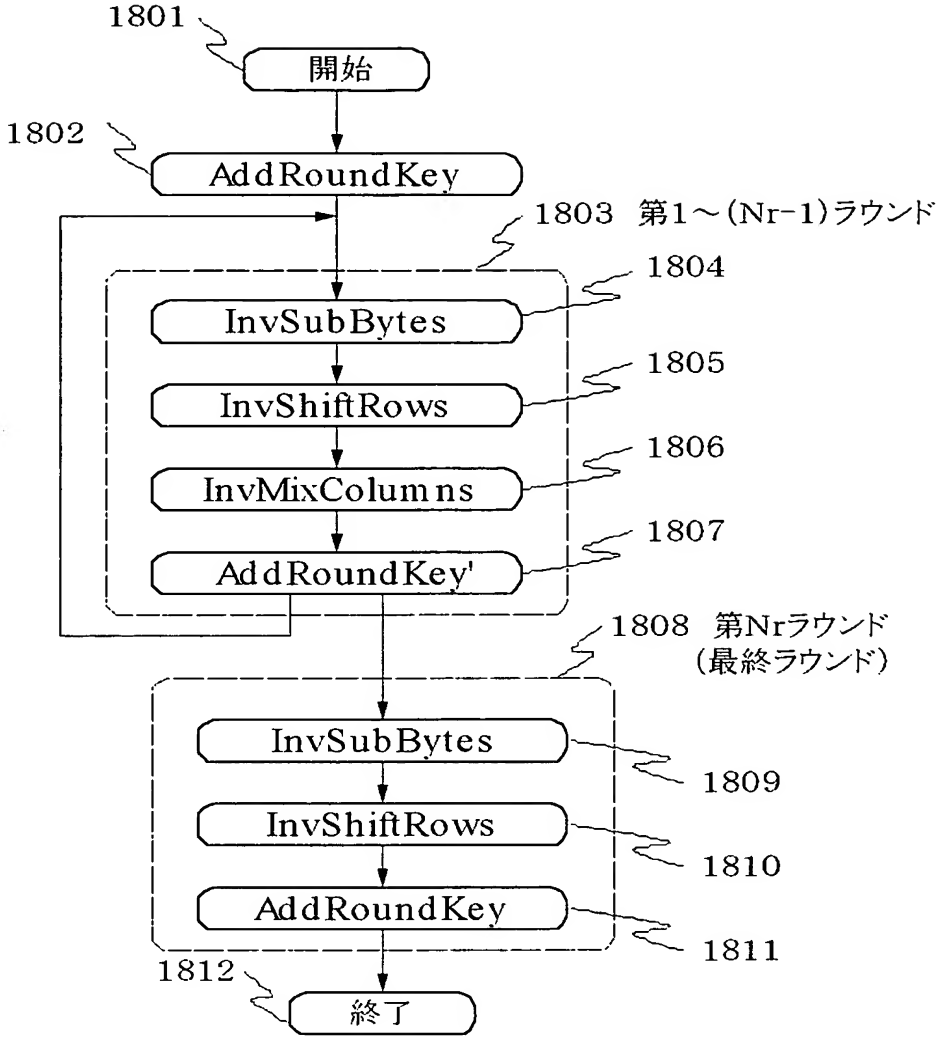
【図２４】


S'0,0 S'0,1 S'0,2 S'0,3
S'1,0 S'1,1 S'1,2 S'1,3
S'2,0 S'2,1 S'2,2 S'2,3
S'3,0 S'3,1 S'3,2 S'3,3
1602
ガロア体上の加算
S-box･{01}
S-box･{02}
S-box･{03}
1601
S-boxテーブル引き
S0,0 S0,1 S0,2 S0,3
S1,0 S1,1 S1,2 S1,3
S2,0 S2,1 S2,2 S2,3
S3,0 S3,1 S3,2 S3,3

【図２５】


ビット長
8
拡張S-box0
拡張S-box1
拡張S-box2
拡張S-box3
1701
拡張S-box
32
ビット長
1702
ビット
31..24
ビット
23..16
ビット
15..8
ビット
7..0
S-box･{03}
S-box･{01}
S-box･{02}
S-box･{01}
S-box･{01}
S-box･{01}
S-box･{02}
S-box･{03}
S-box･{01}
S-box･{01}
S-box･{02}
S-box･{03}
S-box･{02}
S-box･{01}
S-box･{03}
S-box･{01}
1703
ガロア体加算器
S'0,0
S'0,1
S'0,2
S'0,3
S'1,0
S'1,1
S'1,2
S'1,3
S'2,0
S'2,1
S'2,2
S'2,3
S'3,0
S'3,1
S'3,2
S'3,3

【図２６】


1801
開始
1802
AddRoundKey
1803　第1～(Nr-1)ラウンド
1804
InvSubBytes
1805
InvShiftRows
1806
InvMixColumns
1807
AddRoundKey'
1808　第Nrラウンド
(最終ラウンド)
InvSubBytes
1809
InvShiftRows
1810
AddRoundKey
1811
1812
終了

【書類名】　要約書

【要約】

【課題】　ＡＥＳ暗号処理回路の性能を保ちつつ、換字テーブル（Ｓ－ｂｏｘ）の容量を削減する。

【解決手段】　列マルチプレクサ１０２、行マルチプレクサ１０４により、入力ステート１０１上の８ビットの１要素が選択される。選択された要素は、Ｓ－ｂｏｘテーブル１０５により換字処理され、ガロア体乗算器１０７に入力される。ガロア体乗算器１０７により、Ｓ－ｂｏｘテーブル１０５の出力と係数テーブル１０６出力とを４並列乗算し、３２ビット出力を演算結果レジスタ１０８に格納する。演算結果レジスタ１０８の出力は、ガロア体加算器１０９により、累算レジスタ１１０と加算され累算レジスタ１１０に格納される。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０１８８４５
受付番号	５０３００１３２４８７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　１月２９日

＜認定情報・付加情報＞

【提出日】　平成15年 1月28日

次頁無

特願２００３－０１８８４５

出願人履歴情報

識別番号　［０００００４２３７］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社